Red Hat Directory Server 7.1

Red Hat Directory Server Installation Guide

Red Hat Directory Server 7.1: Red Hat Directory Server Installation Guide
Copyright © 2005 Red Hat, Inc.

Red Hat, Inc.

1801 Varsity Drive
Raleigh NC 27606-2072 USA
Phone: +1 919 754 3700
Phone: 888 733 4281
Fax: +1 919 754 3701
PO Box 13588
Research Triangle Park NC 27709 USA

rhds-ig(EN)-7.1-Print-RHI (2005-11-17T16:20-0800)
Copyright © 2001 Sun Microsystems, Inc. Used by permission. Copyright © 2005 by Red Hat, Inc. All rights reserved. This material may be distributed only subject to the terms and conditions set forth in the Open Publication License, V1.0 or later (the latest version is presently available at http://www.opencontent.org/openpub/).
Distribution of substantively modified versions of this document is prohibited without the explicit permission of the copyright holder.
Distribution of the work or derivative of the work in any standard (paper) book form for commercial purposes is prohibited unless prior permission is obtained from the copyright holder.
Red Hat and the Red Hat "Shadow Man" logo are registered trademarks of Red Hat, Inc. in the United States and other countries.
All other trademarks referenced herein are the property of their respective owners.
The GPG fingerprint of the security@redhat.com key is:
CA 20 86 86 2B D6 9D FC 65 F6 EC C4 21 91 80 CD DB 42 A6 0E

Table of Contents

About This Guide ..... **i**
1. Prerequisite Reading i
2. Directory Server Overview i
3. Related Information i
1. Preparing for a Directory Server Installation **1**
1.1. Installation Components 1
1.2. Configuration Decisions 1
1.2.1. Choosing Unique Port Numbers 2
1.2.2. Creating a New Server Root 2
1.2.3. Deciding the User and Group for Your Servers 3
1.2.4. Defining Authentication Entities 3
1.2.5. Determining Your Directory Suffix 4
1.2.6. Determining the Location of the Configuration Directory 4
1.2.7. Determining the Location of the User Directory 5
1.2.8. Determining the Administration Domain 5
1.3. Installation Process Overview 6
1.3.1. Selecting an Installation Process 6
1.3.2. Migration Process 7
1.3.3. Installing the Software 7
1.3.4. Starting the ns-slapd Process 8
1.4. Installation Privileges 8
2. Computer System Requirements **9**
2.1. Summary of Supported Platforms 9
2.1.1. 32-bit Process 9
2.1.2. 64-bit Process 10
2.2. Hardware Requirements 11
2.3. Operating System Requirements 12
2.3.1. `dsktune` Utility 12
2.3.2. Red Hat Enterprise Linux Server Operating System 12
2.3.3. HP-UX 11i Operating System 15
2.3.4. Sun Solaris 9 Operating System 17
2.3.5. DNS and NIS Requirements 20
2.3.6. Installing the JRE 20
3. Using Express and Typical Installation **23**
3.1. Installing on Solaris and HP-UX using an Express Installation 23
3.2. Installing on Solaris and HP-UX using a Typical Installation 24
3.3. Installing on Red Hat Enterprise Linux using an Express Installation 26
3.4. Installing on Red Hat Enterprise Linux Using a Typical Installation 27
4. Silent Installation and Instance Creation **31**
4.1. Using Silent Installation 31
4.1.1. Silent Installation on Red Hat Enterprise Linux 31
4.1.2. Preparing Silent Installation Files 32
4.1.3. Specifying Silent Installation Directives 35
4.2. Using Silent Instance Creation 41
5. Post Installation **43**
5.1. Launching the Help System 43
5.2. Populating the Directory Tree 43

6. Migrating from Previous Versions **45**
6.1. Migration Overview 45
6.2. Migration Prerequisites 46
6.3. Migration Procedure 46
6.3.1. Migrating a Standalone Server 47
6.3.2. Migrating a 6.x Replicated Site 53
6.3.3. Migrating a 6.x Multi-Master Deployment 54
6.3.4. Managing Console Failover 55
6.4. Upgrading from Directory Server 7.x Versions 56
6.4.1. Before You Begin 56
6.4.2. Upgrading 57
6.4.3. After You Upgrade 57
7. Troubleshooting **59**
7.1. Running `dsktune` 59
7.2. Common Installation Problems 61
Glossary **65**
Index **89**

About This Guide

Welcome to Red Hat Directory Server (Directory Server). This manual provides a high-level overview of design and planning decisions you need to make before installing the Directory Server and describes the different installation methods that you can use.

This preface contains the following sections:

- Section 1 *Prerequisite Reading*
- Section 2 *Directory Server Overview*
- Section 3 *Related Information*

1. Prerequisite Reading

Before you install Directory Server, we recommend that you read the *Red Hat Directory Server Deployment Guide*. This guide covers key concepts on how to design and plan your directory service.

After you finish planning your directory service, follow the steps in this installation guide to install the Directory Server and its related software components.

2. Directory Server Overview

The major components of Directory Server include:

- An LDAP server - The core of the directory service, provided by the ns-slapd daemon, and compliant with the LDAP v3 Internet standards.
- Directory Server Console - An improved management console that dramatically reduces the effort of setting up and maintaining your directory service. The directory console is part of Red Hat Console, the common management framework for LDAP directory services.
- SNMP Agent - Permits you to monitor your directory server in real time using the Simple Network Management Protocol (SNMP).
- Online backup and restore - Allows you to create backups and restore from backups while the server is running.

3. Related Information

The document set for Directory Server also contains the following guides:

- *Red Hat Directory Server Administration Guide*. Contains procedures for the day-to-day maintenance of your directory service. Includes information on configuring server-side plug-ins.
- *Red Hat Directory Server Deployment Guide*. Provides an overview for planning your deployment of the Directory Server. Includes deployment examples.
- *Red Hat Directory Server Configuration, Command, and File Reference*. Contains information about using the command-line scripts shipped with Directory Server.
- *Red Hat Directory Server Scheme Reference*. Contains information about the Directory Server schema.
- *Red Hat Directory Server Plug-in Programmer's Guide*. Describes how to write server plug-ins in order to customize and extend the capabilities of Directory Server.

- *Red Hat Directory Server Gateway Customization Guide*. Introduces Directory Server Gateway and explains how to implement a gateway instance with basic directory look-up functionality. Also contains information useful for implementing a more powerful gateway instance with directory authentication and administration capability.
- *Red Hat Directory Server Org Chart*. Introduces the Red Hat Directory Server Org Chart application and explains how to integrate it with an instance of Directory Server.
- *Red Hat Directory Server DSML Gateway Guide*. Introduces the Red Hat Directory Server DSML Gateway function and explains how to customize it for use as an independent gateway.

For a list of documentation installed with Directory Server, open this file:

```
ServerRoot/manual/en/slapd/index.htm
```

For the latest information about Directory Server, including current release notes, complete product documentation, technical notes, and deployment information, refer to http://www.redhat.com/docs/manuals/dir-server

Chapter 1.

Preparing for a Directory Server Installation

Before you begin installing Red Hat Directory Server (Directory Server), you should have an understanding of the various Directory Server components and the design and configuration decisions you need to make.

To help you prepare for your Directory Server installation, you should be familiar with the concepts contained in the following sections:

- Section 1.1 *Installation Components*
- Section 1.2 *Configuration Decisions*
- Section 1.3 *Installation Process Overview*
- Section 1.4 *Installation Privileges*

The *Red Hat Directory Server Deployment Guide* contains basic directory concepts as well as guidelines to help you design and successfully deploy your directory service. Be sure you understand the concepts presented in this manual before proceeding with the installation process.

1.1. Installation Components

Directory Server contains the following software components:

Red Hat Console

Red Hat Console provides the common user interface for Directory Server applications. From it, you can perform common server administration functions such as stopping and starting servers, installing new server instances, and managing user and group information. Red Hat Console can be installed as a stand-alone application on any machine. You can also install it on your network and use it to manage remote servers.

Red Hat Administration Server

Administration Server is a common front-end to all Directory Servers. It receives communications from **Red Hat Console** and passes those communications on to the appropriate Directory Server instance. Your site will have at least one Administration Server for each Directory Server root.

Directory Server

Directory Server is Red Hat's LDAP implementation. The Directory Server runs as the `ns-slapd` process. This is the server that manages the directory databases and responds to client requests. Directory Server is a required component.

The order in which you install and configure the various components depends on whether you are performing a new installation or an upgrade. See Section 1.3 *Installation Process Overview* for details.

1.2. Configuration Decisions

During Directory Server installation, you are prompted for basic configuration information. Decide how you are going to configure these basic parameters before you begin the installation process. You

are prompted for some or all of following information, depending on the type of installation that you decide to perform:

- Port number; refer to Section 1.2.1 *Choosing Unique Port Numbers*.
- Server root; refer to Section 1.2.2 *Creating a New Server Root*.
- Which users and groups you want to run Directory Server as; refer to Section 1.2.3 *Deciding the User and Group for Your Servers*.
- Your directory suffix; refer to Section 1.2.5 *Determining Your Directory Suffix*.
- Several different user IDs and passwords for authentication; refer to Section 1.2.4 *Defining Authentication Entities*.
- The location of the configuration and user directory servers; refer to Section 1.2.6 *Determining the Location of the Configuration Directory* and Section 1.2.7 *Determining the Location of the User Directory*.
- The administration domain; see Section 1.2.8 *Determining the Administration Domain*.

1.2.1. Choosing Unique Port Numbers

Port numbers can be any number from 1 to 65535. Keep the following in mind when choosing a port number for your Directory Server:

- The standard Directory Server (LDAP) port number is 389.
- Port 636 is reserved for secure LDAP (LDAPS). You can also use LDAP over TLS on the standard LDAP port.

  For information on how to set up LDAP over SSL (LDAPS) for Directory Server, see the *Red Hat Directory Server Administration Guide*.
- Port numbers between 1 and 1024 have been assigned to various services by the Internet Assigned Numbers Authority. Do not use port numbers below 1024 other than 389 or 636 for directory services as they will conflict with other services.
- Directory Server must be run as root if it will listen on either port 389 or 636.
- Make sure the ports you choose are not already in use. Additionally, if you are using both LDAP and LDAPS communications, make sure the port numbers chosen for these two types of access are not identical.

You should use the default directory ports (389 and 636) for the user directory. If your configuration directory is managed by a server instance dedicated to that purpose, you should use some non-standard port for the configuration directory.

1.2.2. Creating a New Server Root

Your server root is the directory where you install your Directory Server. The default server root for Directory Server on Linux is `/opt/redhat-ds/`; on other UNIX servers the directory is `/opt/redhat-ds/servers/`.

The server root must meet the following requirements:

- The server root must be a directory on a local disk drive; you cannot use a networked drive for installation purposes. The file sharing protocols such as AFS, NFS, and SMB do not provide file locking and performance suitable for use by the Directory Server. The server database index files may be damaged if they are not held on a local filesystem.

- The directory must not already exist or must be empty.
- When using tarballs, the server root directory must not be the same as the directory from which you are running the setup program.

By default, the server root directory is /opt/redhat-ds/servers.

1.2.3. Deciding the User and Group for Your Servers

For security reasons, it is always best to run production servers with normal user privileges. That is, you do not want to run Directory Server with root privileges. However, you will have to run Directory Server with root privileges if you are using the default Directory Server ports. If Directory Server is to be started by Administration Server, Administration Server must run either as root or as the same user as Directory Server.

You must therefore decide which user accounts you will use for the following purposes:

- The user and group under which you will run Directory Server.

Note

If you will not be running the Directory Server as root, it is strongly recommended that you create a user account for all directory services. You should not use any existing operating system account and must not use the nobody account. Also, you should create a common group for the directory server files; again, you must not use the nobody group.

- The user and group under which you will run Administration Server.

  For installations that use the default port numbers, this must be root. However, if you use ports over 1024, then you should create a user account for all directory services and run Administration Server as this account.

  As a security precaution, when Administration Server is being run as root, it should be shut down when it is not in use.

Note

On Linux, the group names must not contain spaces.

You should use a common group for all directory services, such as gid `DirectoryServer`, to ensure that files can be shared between servers when necessary, and this GID should be the same across all servers that will be running Directory Server since the Directory Server uses this GID to check permissions. Also the UID of the users as whom the Directory Server will run should be the same on all systems.

Before you can install Directory Server and Administration Server, you must make sure that the user and group accounts you will use exist on your system.

1.2.4. Defining Authentication Entities

As you install Directory Server and Administration Server, you will be asked for various user names, distinguished names (DN), and passwords. This list of login and bind entities will differ depending on the type of installation that you are performing:

Directory Manager DN and password.

The Directory Manager DN is the special directory entry to which access control does not apply. Think of the directory manager as your directory's superuser. (In former releases of Directory Server, the Directory Manager DN was known as the *root DN*).

The default Directory Manager DN is `cn=Directory Manager`. Because the Directory Manager DN is a special entry, the Directory Manager DN does not have to conform to any suffix configured for your Directory Server. Therefore, you must not manually create an actual Directory Server entry that has the same DN as the Directory Manager DN.

The Directory Manager password must be at least 8 characters long and is limited to ASCII letters, digits, and symbols.

Configuration Directory Administrator ID and password.

The configuration directory administrator is the person responsible for managing all directory services accessible through Red Hat Console. If you log in with this user ID, then you can administer any Directory Server that you can see in the server topology area of Red Hat Console.

For security, the configuration directory administrator should not be the same as Directory Manager. The default configuration directory administrator ID is admin.

Administration Server user and password.

You are prompted for this only during custom installations. The Administration Server user is the special user that has all privileges for the local Administration Server. Authentication as this person allows you to administer all the servers stored in the local server root.

The Administration Server user ID and password are used only when the Directory Server is down and you are unable to log in as the configuration directory administrator. The existence of this user ID means that you can access Administration Server and perform disaster recovery activities such as starting Directory Server, reading log files, and so forth. Normally, Administration Server user and password should be identical to the configuration directory administrator ID and password.

1.2.5. Determining Your Directory Suffix

A directory suffix is the directory entry that represents the first entry in a directory tree. You will need at least one directory suffix for the tree that will contain your enterprise's data. It is common practice to select a directory suffix that corresponds to the DNS host name used by your enterprise. For example, if your organization uses the DNS name example.com, then select a suffix of `dc=example,dc=com`.

For more information on planning the suffixes for your directory service, see the *Red Hat Directory Server Deployment Guide*.

1.2.6. Determining the Location of the Configuration Directory

The directory instance that stores the configuration information, such as port numbers, is called the *configuration directory*. The configuration information is stored in the `o=NetscapeRoot` tree, which is used by other Directory Server instances. A single instance of Directory Server can be both the configuration directory and the user directory, but it is recommended that you have a separate instance specifically for this configuration directory. The configuration directory can run on the same computer that hosts the user directory, but, for best performance, it should be located on a separate machine.

If you are installing Directory Server only to support other server applications, then that Directory Server is your configuration directory. If you are installing Directory Server to use as part of a general directory service, then you will have multiple Directory Servers installed in your enterprise, and you

must decide which one will host the configuration directory tree, `o=NetscapeRoot`. You must make this decision before you install any compatible server applications, including Directory Server.

For ease of upgrades, you should use a Directory Server instance that is dedicated to supporting the o=NetscapeRoot tree; this server instance should perform no other function with regard to managing your enterprise's directory data. Also, do not use port 389 for this server instance because doing so could prevent you from installing a Directory Server on that host that can be used for management of your enterprise's directory data.

Because the configuration directory normally experiences very little traffic, you can allow its server instance to coexist on a machine with another more heavily loaded Directory Server instance. However, for very large sites that are installing a large number of server instances, you may want to dedicate a low-end machine to the configuration directory so as not to hurt the performance of your other production servers. Directory Server installations result in write activities to the configuration directory. For large enough sites, this write activity could result in a short-term performance hit to your other directory activities.

Also, as with any directory installation, consider replicating the configuration directory to increase availability and reliability. See the *Red Hat Directory Server Deployment Guide* for information on using replication and DNS round-robins to increase directory availability.

Caution

Corrupting the configuration directory tree can result in the necessity of reinstalling all other Directory Servers that are registered in that configuration directory. Remember the following guidelines when dealing with the configuration directory:

- Always back up your configuration directory after you install a new Directory Server.
- Never change the host name or port number used by the configuration directory.
- Never directly modify the configuration directory tree. Only the setup program should ever modify the configuration.

1.2.7. Determining the Location of the User Directory

Just as the configuration directory is the Directory Server that is used for server administration, the *user directory* is the Directory Server that contains the entries for users and groups in your enterprise.

For most directory installations, the user directory and the configuration directory should be two separate server instances. These server instances can be installed on the same machine, but, for best results, you should consider placing the configuration directory on a separate machine.

Between your user directory and your configuration directory, it is your user directory that will receive the overwhelming percentage of the directory traffic. For this reason, you should give the user directory the greatest computing resources. Because the configuration directory should receive very little traffic, it can be installed on a machine with very low-end resources.

You cannot install a user directory until you have installed a configuration directory somewhere on your network.

1.2.8. Determining the Administration Domain

The administration domain allows you to group servers together logically so that you can more easily distribute server administrative tasks. A common scenario is for two divisions in a company to each

want control of their individual servers. However, you may still want some centralized control of all the servers in your enterprise. Administration domains allow you to meet these conflicting goals.

Administration domains have the following qualities:

- All servers share the same configuration directory, regardless of the domain to which they belong.
- Servers in two different domains may use two different user directories for authentication and user management.
- The configuration directory administrator has complete access to all installed Directory Servers, regardless of the domain to which they belong.
- Each administration domain can be configured with an administration domain owner. This owner has complete access to all the servers in the domain but does not have access to the servers in any other administration domain.
- The administration domain owner can grant individual users administrative access on a server by server basis within the domain.

For many installations, you can have just one administration domain. In this case, choose a name that is representative of your organization. For other installations, you may want different domains because of the demands at your site. In the latter case, try to name your administration domains after the organizations that will control the servers in that domain.

For example, if you are an ISP and you have three customers for whom you are installing and managing Directory Server instances, create three administration domains each named after a different customer.

1.3. Installation Process Overview

You can use one of several installation processes to install Directory Server. Each one guides you through the installation process and ensures that you install the various components in the correct order.

The sections that follow outline the installation processes available, how to upgrade from an earlier release of Directory Server, and how to unpack the software to prepare for installation.

1.3.1. Selecting an Installation Process

You can install Directory Server software using one of the four different installation methods provided in the setup program:

Express Installation

Use an express installation if you are installing for the purposes of evaluating or testing Directory Server. Express installation is described in Section 3.1 *Installing on Solaris and HP-UX using an Express Installation*.

Typical Installation

Use a typical installation if you are performing a normal installation of Directory Server. Typical installation is described in Section 3.2 *Installing on Solaris and HP-UX using a Typical Installation*.

Custom Installation

In Directory Server, the custom installation process is very similar to the typical installation process. The main difference is that the custom installation process allows you to import an LDIF file to initialize the user directory database that is created by default.

Silent Installation

Use a silent installation if you want to script your installation process. This is especially useful for installing multiple replica servers around your enterprise. Silent install is described in Chapter 4 *Silent Installation and Instance Creation*.

Beyond determining which type of installation process you will use, the process for installing Directory Server is as follows:

1. Plan your directory service. By planning your directory tree in advance, you can design a service that is easy to manage and easy to scale as your organization grows. For guidance on planning your directory service, refer to the *Red Hat Directory Server Deployment Guide*.
2. Install your Directory Server as described in this manual.
3. Create the directory suffixes and databases. You do not have to populate your directory now; however, you should create the basic structure for your tree, including all major roots and branch points. For information about the different methods of creating a directory entry, refer to the *Red Hat Directory Server Administration Guide*.
4. Create additional Directory Server instances, and set up replication agreements between your Directory Servers to ensure availability of your data.

1.3.2. Migration Process

Directory Server supports migration from previous releases of Directory Server. The migration process is described in Chapter 6 *Migrating from Previous Versions*.

1.3.3. Installing the Software

Note

Before you install Directory Server, ensure that the host system is brought up to date with the latest patches recommended for Red Hat Enterprise Linux. Because the list of recommended patches changes with time, you must always use http://rhn.redhat.com to keep entitled systems current with the latest recommended patches.

How you install the software depends on whether you have the RPM or a tarball:

1.3.3.1. For RPMs...

If you have the product binaries RPM, install it with:

```
rpm -ivh filename.rpm
```

where `filename` corresponds to the product binaries that you want to install.

1.3.3.2. For tarballs...

If you have obtained Directory Server tarball from the website, you will need to unpack it before beginning installation.

1. Create a new directory for the installation:
   ```
   mkdir ds
   cd ds
   ```
2. Download the product binaries file to the installation directory.
3. Unpack the product binaries file using the following command:
   ```
   gzip -dc filename.tar.gz | tar -xvof -
   ```
   where *filename* corresponds to the product binaries that you want to unpack.

1.3.4. Starting the ns-slapd Process

You will need to write an rc script to start the ns-slapd process, as it does not start automatically when the system boots.

1.4. Installation Privileges

You must install as root if you choose to run the server on a port below 1024, such as the default LDAP ports: 389 and 636 (LDAP). If you choose port numbers higher than 1024, you can install using any valid UNIX login.

Chapter 2.

Computer System Requirements

Before you can install Red Hat Directory Server (Directory Server), you must make sure that the systems on which you plan to install the software meet the minimum hardware and operating system requirements.

Directory Server is compiled as a 64-bit application for some platforms, meaning Directory Server supports deployments with memory cache sizes larger than 4 GB and limited only by available memory.

It is possible to use Directory Server as a 32-bit application on supported 32-bit platforms. On 64-bit platforms, if the memory cache size is smaller than 4 GBs, it is recommended that you run the 32-bit application of Directory Server since this may improve performance. Be sure that you have the correct application for your Directory Server deployment.

These requirements are described in detail for each platform in the following sections:

- Section 2.1 *Summary of Supported Platforms*
- Section 2.2 *Hardware Requirements*
- Section 2.3 *Operating System Requirements*.

2.1. Summary of Supported Platforms

This release of Directory Server is supported on the platforms listed in Table 2-1 and Table 2-3. The sections that follow provide information that is specific to each of the supported platforms:

- Section 2.1.1 *32-bit Process*
- Section 2.1.2 *64-bit Process*

Before you install Directory Server, check the required patches and kernel parameter settings, as described in the sections that follow. Also, ensure that DNS is properly configured on the system, that the system has a static IP address, and that you have installed the proper JRE packages on your system.

2.1.1. 32-bit Process

OS Version	Red Hat Enterprise Linux with relevant upgrades/patches. For details, see Section 2.3.2 *Red Hat Enterprise Linux Server Operating System*.
CPU	500 MHz or higher, compatible with Pentium 3 or higher.
Memory/RAM	256 MBs. However, you should have at least 1 GB of RAM for best performance on large production systems.
Storage Space/Hard Disk	Approximately 300 MBs of disk space for a minimal installation. For production systems, you should plan at least 2 GB to support the product binaries, databases, and log files (log files require 1 GB by default); 4 GB and greater may be required for very large directories.

Other Requirements	You must install as root in order to use well-known port numbers (such as 389) that are less than 1024. If you do not plan to use port numbers less than 1024, you do not need to install as root. If you plan to run as root, you should also install as root and specify nobody as the default run-as user and group.

Table 2-1. Red Hat Enterprise Linux - 32-bit

OS Version	Solaris 9 with relevant patches. For details, see Section 2.3.4 *Sun Solaris 9 Operating System*Sun Solaris 9 Operating System. Solaris bits can run in 32-bit or 64-bit operating system mode.
CPU	UltraSparc-IIi 300Mhz or faster (32 bit).
Memory/RAM	256 MB. However, you should plan for 1 GB of RAM for best performance on large production systems.
Storage Space/Hard Disk	Approximately 300 MBs of disk space for a minimal installation. For production systems, you should plan at least 2 GB to support the product binaries, databases, and log files (log files require 1 GB by default); 4GB and greater may be required for very large directories. To support database files that are larger than 2 GB, the machine must be configured to support large files; you can do this by choosing largefile.
Other Requirements	You must install as root in order to use well-known port numbers (such as 389) that are less than 1024. If you do not plan to use port numbers less than 1024, you do not need to install as root. If you plan to run as root, you should also install as root and specify nobody as the default run-as user and group.

Table 2-2. Sun Solaris Platform Requirements

2.1.2. 64-bit Process

OS Version	HP-UX 11i; must be fully patched. For details, see Section 2.3.3 *HP-UX 11i Operating System*HP-UX 11i Operating System.
CPU	HP 9000 architecture with a PA-RISC 2.0 CPU.
Memory/RAM	256 MB. However, you should plan for 1 GB of RAM for best performance on large production systems.
Storage Space/Hard Disk	Approximately 300 MBs of disk space for a minimal installation. For production systems, you should plan at least 2 GB to support the product binaries, databases, and log files (log files require 1 GB by default); 4 GB and greater may be required for very large directories. To support database files that are larger than 2 GB, the machine must be configured to support large files; you can do this by choosing vxfs filesystem with largefiles option. See the fsadm documentation for more information.

Other Requirements	You must install as root in order to use well-known port numbers (such as 389) that are less than 1024. If you do not plan to use port numbers less than 1024, you do not need to install as root. If you plan to run as root, you should also install as root and specify nobody as the default run-as user and group.

Table 2-3. HP-UX - 64-bit

OS Version	Solaris 9 with relevant patches. For details, see Section 2.3.4 *Sun Solaris 9 Operating System*Sun Solaris 9 Operating System. Solaris can run in 32-bit or 64-bit operating system mode.
CPU	UltraSparc-IIi 300Mhz or faster (64-bit).
Memory/RAM	256 MB. However, you should plan for 1 GB of RAM for best performance on large production systems.
Storage Space/Hard Disk	Approximately 300 MB of disk space for a minimal installation. For production systems, you should plan at least 2 GB to support the product binaries, databases, and log files (log files require 1 GB by default); 4 GB and greater may be required for very large directories. To support database files that are larger than 2 GB, the machine must be configured to support large files; you can do this by choosing largefile.
Other Requirements	You must install as root in order to use well-known port numbers (such as 389) that are less than 1024. If you do not plan to use port numbers less than 1024, you do not need to install as root. If you plan to run as root, you should also install as root and specify nobody as the default run-as user and group.

Table 2-4. Sun Solaris Platform Requirements

2.2. Hardware Requirements

On all platforms, you need:

- Roughly 200 MB of disk space for a minimal installation. For production systems, you should plan at least 2 GB to support the product binaries, databases, and log files (log files require 1 GB by default); 4 GB and greater may be required for very large directories.
- 256 MB of RAM. However, you should plan for 1 GB of RAM for best performance on large production systems.

The table below contains some guidelines for disk space and memory requirements depending on the number of entries managed by your Directory Server. This assumes entries in the LDIF file are approximately 100 bytes in size and only the recommended indexes are configured. If you are using larger entries, make sure that at least four times the size of the LDIF file is available on disk.

Number of Entries	Disk Space and Memory Required
10,000 - 250,000 entries	Free disk space: 2 GB Free memory: 256 MB

Number of Entries	Disk Space and Memory Required
250,000 - 1,000,000 entries	Free disk space: 4 GB Free memory: 512 MB
Over 1,000,000 entries	Free disk space: 8 GB Free memory: 1 GB

2.3. Operating System Requirements

This section contains information on operating-system versions and patches required for installing Directory Server:

- Section 2.3.1 `dsktune` *Utility*
- Section 2.3.2 *Red Hat Enterprise Linux Server Operating System*
- Section 2.3.3 *HP-UX 11i Operating System*
- Section 2.3.4 *Sun Solaris 9 Operating System*
- Section 2.3.5 *DNS and NIS Requirements*
- Section 2.3.6 *Installing the JRE*

2.3.1. `dsktune` Utility

Directory Server provides a utility named `dsktune` that can help you verify whether you have the appropriate patches installed on your system. The utility also provides useful information and advice on how to tune your kernel parameters for best performance.

To enable you to run `dsktune` before installing the Directory Server, the utility is placed, along with the setup program, in the directory where you unpack product binaries. The setup program allows specifying of a pre-pre-installation program to be run before the Directory Server installation begins; in the slapd.inf file, a new field named `PrePreInstall` is defined for specifying the path to the executable, which must be relative to the setup program. By default, the PrePreInstall field is set to the `dsktune` utility path, enabling you to run the utility as a part of the Directory Server installation.

After you have installed the Directory Server, you can find the utility in this directory:

serverRoot`/bin/slapd/server`

For information on running `dsktune`, see Chapter 7 *Troubleshooting*.

Tip

Tip: It is strongly recommended that you run the `dsktune` utility. Kernel parameters make a significant performance difference; for example, in some cases on HP-UX systems, Directory Server may not run on stock kernel parameters.

2.3.2. Red Hat Enterprise Linux Server Operating System

If you plan to install Directory Server on a machine running the Red Hat Enterprise Linux operating system, follow the recommendations outlined in these sections:

- Section 2.3.2.1 *Verifying Disk Space Requirements*
- Section 2.3.2.2 *Verifying Required System Modules*
- Section 2.3.2.3 *Installing System Patches*
- Section 2.3.2.4 *Tuning the System*
- Section 2.3.2.5 *Installing Third-Party Utilities*.

In addition to these recommendations, be sure to check the Red Hat website for the latest information pertaining to your Linux version: http://www.redhat.com/apps/support/

2.3.2.1. Verifying Disk Space Requirements

Ensure that you have sufficient disk space before downloading the software:

- Download drive: 120 MB
- Installation drive: 2 GB

2.3.2.2. Verifying Required System Modules

Directory Server is certified to work on:

- The Intel Pentium series processors [i686].
- The default kernel/glibc revisions that comes along with Red Hat Enterprise Linux and the other kernel revisions with their corresponding glibc revisions as mentioned below.

  Red Hat Enterprise Linux 3:

  - Default kernel: kernel-2.4.21-3.EL
  - Kernel used for certification: kernel-2.4.21-27.0.2.EL
  - Default glibc: glibc-2.3.2-95.3
  - glibc used for certification: glibc-2.3.2-95.33
  - Required Filesytem: ext3 (LARGEFILES support enabled) filesystem has been used for the certification process.

  Red Hat Enterprise Linux 4:

  - Default kernel: kernel-2.6.9-5_EL
  - Kernel used for certification: kernel-2.6.9-5.0.5.EL
  - Default glibc: glibc-2.3-4.2
  - glibc used for certification: glibc-2.3.2-95.30
  - Required Filesytem: ext3 (LARGEFILES support enabled) filesystem has been used for the certification process.

- With certain installed RPM packages on Red Hat Enterprise Linux, the server does not start.

Tip

Red Hat Enterprise Linux is distributed with two RPM packages for glibc, one for 386 processors and higher, the other for 486 or Pentium processors and higher. The 386 package has no NPTL support. If the 386 package is installed on a machine, you lose NPTL support. Once this has happened, it is very hard to detect because `rpm -q` reports the package name and version without the architecture tag.

To determine which RPM package is installed, run the following command:

```
getconf GNU_LIBPTHREAD_VERSION
```

2.3.2.3. Installing System Patches

Directory Server has been certified on Red Hat Enterprise Linux with the following kernel and glibc versions:

- Red Hat Enterprise Linux 3: kernel revisions 2.4.21-4.EL (kernel-2.4.21-4.EL.i686.rpm) and glibc version 2.3.2-95.20 (glibc-2.3.2-95.20.i686.rpm).
- Red Hat Enterprise Linux 4: default kernel kernel-2.6.9-5_EL (with certification on kernel-2.6.9-5.0.5.EL) and glibc version glibc-2.3-4.2 (with certification on glibc-2.3.2-95.30).

It is recommended that you use these kernel and glibc versions. If the machine is a single CPU machine, the corresponding kernel would be of the form `kernel-x.x.x.x`. If the machine is a multi-CPU machine, the corresponding kernel would be of the form `kernel-smp-x.x.x.x`.

You can get the list of software installed on your system, including patches, by running: `rpm -qa`

2.3.2.4. Tuning the System

This section contains some basic system tuning information. Changing any of the following kernel-tuning parameters requires a system reboot.

- NFS Tuning: This tuning is recommended if you are using Directory Server to write to NFS mounted drives. On Linux, NFS is typically recommended to be done over TCP and not over UDP. Make the following change to the `/etc/rc.d/init.d/autofs` file:
  ```
  + localoptions='rsize=8192,wsize=8192,vers=3,tcp'
  ```
- TCP Tuning: You can increase the number of available local system ports available by running this command:
  ```
  echo "1024 65000" > /proc/sys/net/ipv4/ip_local_port_range
  ```
  Make this change permanent by adding this line to the `/etc/sysctl.conf` file:
  ```
  net.ipv4.ip_local_port_range = 1024 65000
  ```
- File Tuning: Check the current maximum number of files that can be stored on your system:
  ```
  cat /proc/sys/fs/file-max
  ```
  If this number is less than 64000, increase it with this command:
  ```
  echo 64000 > /proc/sys/fs/file-max
  ```
  Make the change permanent by adding this line to the `/etc/sysctl.conf` file:
  ```
  fs.file-max = 64000
  ```
- Then, you need to increase the maximum number of open files. Add the following line to the `/etc/security/limits.conf` file:
  ```
  *        -        nofile        8192
  ```

- Lastly, edit the file `/etc/pam.d/system-auth` to include this line if it does not already exist:
  `session required /lib/security/$ISA/pam_limits.so`

You must log out and then log back in for changes in the `limits.conf` file to take effect.

2.3.2.5. Installing Third-Party Utilities

You need the gunzip utility to unpack the Directory Server software. The GNU gzip and gunzip programs are described in more detail at http://www.gnu.org/software/gzip/gzip.html and can be obtained from many software distribution sites.

You may need Adobe Acrobat Reader to read the documentation. If you do not have it installed, you can download it from http://www.adobe.com/products/acrobat/readstep2.html.

2.3.3. HP-UX 11i Operating System

This section contains the following information:

- Section 2.3.3.1 *Verifying Disk Space Requirements*
- Section 2.3.3.2 *Verifying Required System Modules*
- Section 2.3.3.3 *Installing Patches*
- Section 2.3.3.4 *Tuning the System*
- Section 2.3.3.5 *Installing Third-Party Utilities*.

2.3.3.1. Verifying Disk Space Requirements

Ensure that you have sufficient disk space before downloading the software.

- Download drive: 120 MB
- Installation drive: 2 GB

2.3.3.2. Verifying Required System Modules

Directory Server is not supported on HP-UX 10 or earlier versions. The minimum system module required is HP-UX 11i. Directory Server may only be used on a 64-bit HP-UX 11i environment as a 64-bit process and may contain up to 8 GB of process memory.

For best results, Directory Server requires an HP 9000 architecture with a PA-RISC 2.0 CPU.

2.3.3.3. Installing Patches

Before you install Directory Server, ensure that the host system is updated with the latest patches recommended by the operating-system vendor. Because the list of recommended patches changes with time, you must always check the operating system vendor's site for a list of patches that you may need to install. Listed below are two URLs to aid you in this effort:

- http://welcome.hp.com/country/us/eng/support.htm
- http://www.hp.com/products1/unix/java/

Here are some recommendations:

- For HP-UX 11i, install the latest HP-UX 11i Quality Pack (GOLDQPK11i) patch from June 2004 or later. For details, refer to http://www.software.hp.com/SUPPORT_PLUS/qpk.html.
- The PHSS_30966: ld(1) and linker tools cumulative patch is critical before installation of Directory Server.
- The following patches are recommended:

GOLDAPPS11i:	B.11.11.0406.5 Gold Applications Patches for HP-UX 11i v1, June 2004
GOLDBASE11i:	B.11.11.0406.5 Gold Base Patches for HP-UX 11i v1, June 2004

- Run the `dsktune` utility to see if you need to install any other patches. The utility helps you to verify whether you have the appropriate patches installed on your system and provides useful information and advice on how to tune your kernel parameters for best performance. For information on the `dsktune` utility, see Section 2.3.1 *`dsktune` Utility*.

2.3.3.4. Tuning the System

Set your kernel parameters as follows:

- Set maxfiles to 1024.
- Set nkthread to 1328; nkthread is a computed value: (((NPROC*7)/4+16).
  - Set max_thread_proc to 512.
  - Set maxusers to 64.
  - Set maxuprc to 512.
  - Set nproc to 750.

Typically, client applications that do not properly shut down the socket cause it to linger in a TIME_WAIT state. To prevent this, you should consider changing the TIME_WAIT setting to a reasonable value. For example, setting

```
ndd -set /dev/tcp tcp_time_wait_interval 60000
```

limits the `TIME_WAIT` state of sockets to 60 seconds.

You also need to turn on large file support in order for Directory Server to work properly. To change an existing filesystem (from one that has no large files to one that accepts large files):

1. Unmount the system using the umount command:
   ```
   umount /export
   ```
2. Create the large filesystem:
   ```
   fsadm -F vxfs -o largefiles /dev/vg01/rexport
   ```
3. Remount the filesystem:
   ```
   /usr/sbin/mount -F vxfs -o largefiles /dev/vg01/export
   ```

For additional information and recommendations about setting these parameters, consult your operating-system documentation.

2.3.3.5. Installing Third-Party Utilities

You need the gunzip utility to unpack the Directory Server software. The GNU gzip and gunzip programs are described in more detail at http://www.gnu.org/software/gzip/gzip.html and can be obtained from many software distribution sites.

You may need Adobe Acrobat Reader to read the documentation. If you do not have it installed, you can download it from http://www.adobe.com/products/acrobat/readstep2.html.

2.3.4. Sun Solaris 9 Operating System

If you plan to install Directory Server on a machine running the Solaris 9 operating system, follow the recommendations outlined in these sections:

- Section 2.3.4.1 *Verifying Disk Space Requirements*
- Section 2.3.4.2 *Verifying Required System Modules*
- Section 2.3.4.3 *Installing Patches*
- Section 2.3.4.4 *Tuning the System*
- Section 2.3.4.5 *Setting File Descriptors*
- Section 2.3.4.6 *Tuning TCP Parameters*.

In addition to these recommendations, be sure to check Sun's website for the latest information pertaining to your operating system version. For example, you should read the *Solaris Operating Environment Security Sun Blueprint* at http://www.sun.com/blueprints/0100/security.pdf for advice on guarding against potential security threats.

Below are two URLs that you may find useful:

- http://docs.sun.com
- http://sunsolve.sun.com

2.3.4.1. Verifying Disk Space Requirements

Ensure that you have sufficient disk space before downloading the Directory Server software.

- Download drive: 120 MB
- Partition containing /opt/redhat-ds: 2 GB

2.3.4.2. Verifying Required System Modules

Directory Server requires the use of an UltraSPARC (SPARC v9) processor, as this processor includes support for high-performance and multiprocessor systems. Earlier SPARC processors are not supported.

If you run Directory Server on a 64-bit Sun Solaris 8 UltraSPARC machine, it runs as a 32-bit application.

2.3.4.3. Installing Patches

You must use Solaris 9 with the Sun recommended patches. The Sun recommended patch clusters can be obtained from your Solaris support representative or from the http://sunsolve.sun.com site.

Solaris patches are identified by two numbers; for example, 112233-04. The first number (112233) identifies the patch itself. The second number identifies the version of the patch; in the example above, the patch is version number 04.

Table 2-5 provides the list of Solaris 9 patches that were used during the testing of this release of Directory Server. You must install these patches on your machine before installing the Directory Server product. (The command `showrev -p` lists the patches that have been installed on your machine.)

Also, keep in mind that Directory Server provides a utility named `dsktune` that can help you verify whether you have the appropriate patches installed on your system. For details, see Section 2.3.1 *`dsktune` Utility*

In addition to the patches listed in Table 2-5 and the patches identified by the `dsktune` utility, we recommend that you check the operating system vendor's web site for information on installing the latest version of the patch clusters to benefit from the latest fixes.

You must reboot your machine after installing the patches.

112998-03:	SunOS 5.9: patch /usr/sbin/syslogd
112875-01:	SunOS 5.9: patch /usr/lib/netsvc/rwall/rpc.rwalld
113146-04:	SunOS 5.9: Apache Security Patch
113068-05:	SunOS 5.9: hpc3130 Patch
112963-14:	SunOS 5.9: linker patch
113273-08:	SunOS 5.9: /usr/lib/ssh/sshd Patch
112233-12:	SunOS 5.9: Kernel Patch
112964-08:	SunOS 5.9: /usr/bin/ksh Patch
112808-06:	CDE1.5: Tooltalk Patch
113279-01:	SunOS 5.9: klmmod Patch
113278-07:	SunOS 5.9: NFS Daemon Patch
113023-01:	SunOS 5.9: Broken preremove scripts in S9 ALC packages
112764-07:	SunOS 5.9: Sun Quad FastEthernet qfe driver
113033-04:	SunOS 5.9: patch /kernel/drv/isp and /kernel/drv/sparcv9/isp
112601-09:	SunOS 5.9: PGX32 Graphics
113923-02:	X11 6.6.1: security font server Patch
112817-18:	SunOS 5.9: Sun GigaSwift Ethernet 1.0 driver Patch
113718-02:	SunOS 5.9: usr/lib/utmp_update Patch
114135-01:	SunOS 5.9: at utility Patch
112834-04:	SunOS 5.9: patch scsi
112907-03:	SunOS 5.9: libgss Patch
113319-19:	SunOS 5.9: libnsl nispasswd patch

112785-43:	X11 6.6.1: Xsun Patch
112970-07:	SunOS 5.9: patch libresolv
112951-09:	SunOS 5.9: patchadd and patchrm Patch
113277-24:	SunOS 5.9: st, sd, and ssd Patch
113579-06:	SunOS 5.9: ypserv/ypxfrd Patch
112908-14:	SunOS 5.9: krb5 shared object Patch
113073-14:	SunOS 5.9: ufs and fsck Patch

Table 2-5. Solaris 9 Patch List

2.3.4.4. Tuning the System

Basic Solaris tuning guidelines are available from several books, including *Sun Performance and Tuning: Java and the Internet* (ISBN 0-13-095249-4). Advanced tuning information is available in the *Solaris Tunable Parameters Reference Manual* (816-7137), which can be obtained from http://docs.sun.com/db/doc/816-7137.

2.3.4.5. Setting File Descriptors

The system-wide maximum file descriptor table size setting limits the number of concurrent connections that can be established to Directory Server. The governing parameter, *rlim_fd_max*, is set in the `/etc/system` file. By default, if this parameter is not present, the maximum is 1024. It can be raised to 4096 by adding a line such as `set rlim_fd_max=4096` to `/etc/system` and rebooting the system.

Caution

This parameter should not be raised above 4096 without first consulting your Sun Solaris support representative since it may affect the stability of the system.

You should also set the soft limit for file descriptors:

```
ulimit -n in csh limit desc 1024
```

Use the `dsktune` utility (see Section 2.3.1 *`dsktune` Utility*) to learn about the hard and soft limits for file descriptors.

2.3.4.6. Tuning TCP Parameters

By default, the TCP/IP implementation in a Solaris kernel is not correctly tuned for Internet or Intranet services. The following /dev/tcp tuning parameters should be inspected and, if necessary, changed to fit the network topology of the installation environment.

The *`tcp_time_wait_interval`* in Solaris 9 specifies the number of milliseconds that a TCP connection is held in the kernel's table after it has been closed. If its value is above 30000 (30 seconds) and the directory is being used in a LAN, MAN, or under a single network administration, it should be reduced by adding a line to the `/etc/init.d/inetinit` file similar to the following:

```
ndd -set /dev/tcp tcp_time_wait_interval 30000
```

The *tcp_conn_req_max_q0* and *tcp_conn_req_max_q* parameters control the maximum backlog of connections that the kernel accepts on behalf of the Directory Server process. If the directory is expected to be used by a large number of client hosts simultaneously, these values should be raised to at least 1024 by adding a line to the `/etc/init.d/inetinit` file similar to the following:

```
ndd -set /dev/tcp tcp_conn_req_max_q0 1024
ndd -set /dev/tcp tcp_conn_req_max_q 1024
```

The *tcp_keepalive_interval* specifies the interval in seconds between keepalive packets sent by Solaris for each open TCP connection. This can be used to remove connections to clients that have become disconnected from the network.

The *tcp_rexmit_interval_initial* value should be inspected when performing server performance testing on a LAN or high speed MAN or WAN. For operations on the wide area Internet, its value need not be changed.

The `tcp_smallest_anon_port` controls the number of simultaneous connections that can be made to the server. When rlim_fd_max has been increased to above 4096, this value should be decreased by adding a line to the `/etc/init.d/inetinit` file similar to the following :

```
ndd -set /dev/tcp tcp_smallest_anon_port 8192
```

2.3.5. DNS and NIS Requirements

Prior to installation, it is necessary to have configured the DNS resolver or NIS domain name.

The DNS resolver is typically set by the file `/etc/resolv.conf`. However, also check the file `/etc/nsswitch.conf` and, on Solaris, `/etc/netconfig` to ensure that the DNS resolver is used for name resolution.

If you are not already using NIS, you also need to set the default NIS domain name. Typically, this is done by placing the NIS domain name in the file `/etc/defaultdomain` and rebooting or by using the domainname command.

2.3.6. Installing the JRE

Not necessary for Red Hat Enterprise Linux.

Necessary Java JRE libraries are not bundled with Directory Server. They must be downloaded and extracted separately prior to installation. If they are not, installation fails.

Note

It is recommended that you use the test versions of the Java JRE package; HP was tested with j2re1.4.2_07; Sun was tested with j2re1.4.2_04. Use the Solaris 9 32-bit package for both 32-bit and 64-bit Sun installations.

Obtain the OS-appropriate Java libraries from either http://www.java.com or http://www.hp.com/products1/unix/java/

Extract these files in a separate directory from your Directory Server installation, such as /export/redhat/jre.

Make sure the JRE package is executable, then run the file. For example:

```
chmod a+x j2re-1_4_2_04-solaris-sparc.sh
./j2re-1_4_2_05-solaris-sparc.sh
```

This extracts a new JRE directory called j2re.1.4.2_05.

When you first run setup, you are asked for the JRE path. Fill in the absolute path as follows:

```
/export/redhat/jre/j2re1.4.2_04
```

If you are doing a silent installation, set the JRE path as an environment variable before running setup:

```
export NSJRE=/tmp/java/jre/j2re1.4.2_04
```

Chapter 3.
Using Express and Typical Installation

This chapter describes how to perform basic installation activities. This chapter contains the following sections:

- Section 3.1 *Installing on Solaris and HP-UX using an Express Installation*
- Section 3.2 *Installing on Solaris and HP-UX using a Typical Installation*
- Section 3.4 *Installing on Red Hat Enterprise Linux Using a Typical Installation*.

3.1. Installing on Solaris and HP-UX using an Express Installation

Use express installation if you are installing Directory Server to evaluate or test the product. Because express installation does not offer you the choice of selecting your server port number or your directory suffix, you should not use it for production installations.

To perform an express installation, do the following:

1. Log in as root (root login is required for express installation).
2. Create a new directory:
   ```
   mkdir ds
   cd ds
   ```
3. If you have not already done so, download the product binaries file to the installation directory.
4. Unpack the product binaries file using the following command:
   ```
   gunzip -dc filename.tar.gz | tar -xvof -
   ```
   where *filename* corresponds to the product binaries you want to unpack.
5. Run the setup program. You can find it in the directory in which you untarred or unzipped the binary files.
6. Issue the following command:
   ```
   ./setup
   ```
7. You will need to download a copy of the JRE for use with Directory Server. When asked for the location of the unpackaged JRE, enter the full path to the location of your downloaded JRE. See Section 2.3.6 *Installing the JRE*.
8. Once the JRE is installed, `dsktune` will run, providing valuable host-tuning information. Enter **`yes`** once the machine has been tuned.
9. Select [yes] to continue with installation, then select `yes` to agree to the license.
10. When you are asked what you would like to install, select the default, **Red Hat Servers**.
11. When you are asked what type of installation you would like to perform, select **Express Installation**.
12. For the server root or destination directory, enter a full path to the location where you want to install your server.

    The location that you enter must be some directory other than the directory from which you are running the setup program. Also, the name of the directory where you install files must not

contain any space characters. If the directory that you specify does not exist, the setup program creates it for you.

13. Choose **All** to install all components.
14. For the user and group to run the servers, enter the identity as whom you want this server to run. For more information on the user and groups that you should use when running your servers, see Section 1.2.3 *Deciding the User and Group for Your Servers*.
15. For configuration directory administrator ID and password, enter the name and password as whom you will log in when you want to authenticate to the **Console** with full privileges (think of this as the root or superuser identity for the **Red Hat Console**).

The server is then unpackaged, minimally configured, and started. You are told on what host and port number the server is listening:

- The Directory Server is listening on port 389 (the default).
- The server is configured to use the following suffixes:

dc=*your_machine's_DNS_domain_name*

If your machine is named `test.example.com`, then you will have the suffix `dc=example,dc=com` configured for this server.

o=NetscapeRoot

Do not modify the contents of the directory under the `o=NetscapeRoot` suffix. Either create data under the first suffix or create a new suffix to be used for this purpose. For details on how to create new suffixes for your Directory Server, see the *Red Hat Directory Server Administration Guide*.

3.2. Installing on Solaris and HP-UX using a Typical Installation

Most first time installations of Directory Server can be performed using the `Typical Installation` option of the setup program.

To perform a typical installation:

1. Log in as root.
2. Create a new directory:
```
mkdir ds
cd ds
```
3. If you have not already done so, download the product binaries file to the installation directory.
4. Unpack the product binaries file using the following command:
```
gunzip -dc filename.tar.gz | tar -xvof -
```
where *filename* corresponds to the product binaries that you want to unpack.
5. Run the setup program. You can find it in the directory in which you untarred or unzipped the binary files. Issue the following command from the installation directory:
```
./setup
```
6. The setup program asks if you would like to proceed with the setup. Press [Enter] to respond with the default (the default for this prompt is **Yes**) or press **N** if you would like to exit the setup program.
7. Next, the setup program asks you if you agree to the license terms. Press **y** to agree with the license terms.

8. When you are asked what you would like to install, press [Enter] to select the default, Red Hat Servers.
9. When you are asked what type of installation you would like to perform, press [Enter] to select the default, `Typical Installation`.
10. For server root, enter a full path to the location where you want to install your server.

    The location that you enter must be some directory other than the directory from which you are running setup. Also, the name of the directory where you install files must not contain any space characters. If the directory that you specify does not exist, setup creates it for you.

    By default, the setup program provides the following path:
    `/opt/redhat/servers`

    If you want to install the software into this directory tree, press [Enter]; otherwise, supply your own path.
11. For the Server Products Core Components, Directory Suite, Administration Services, nsPerl, and PerLDAP, press [Enter] to select the default (all components).
12. Press [Enter] to select all of the Server Products Core Components.
13. Press [Enter] to select all the Directory Suite components.
14. Press [Enter] to select all of the Administration Services components (**Red Hat Administration Server** and the **Administration Server Console**).
15. For the hostname, enter a fully qualified hostname.

    Caution

    The default hostname may be incorrect if the installer cannot locate a DNS name in your system. For example, you might not have a DNS name if your system uses NIS.

    The hostname must be a fully qualified host and domain name. If the default hostname is not a fully qualified host and domain name, installation will fail. Refer to Section 7.2 *Common Installation Problems* for more information about entering a fully qualified domain name.
16. The setup program then asks you for the `System User` and the `System Group` names. Enter the identity under which you want the servers to run.

    For more information on the user and group names that you should use when running your servers, refer to Section 1.2.3 *Deciding the User and Group for Your Servers*.
17. For the configuration directory, select the default if this directory will host your `o=NetscapeRoot` tree. Otherwise, enter **`yes`**. You will then be asked for the contact information for the configuration directory.

    If the server you are currently installing is not the configuration directory, then the configuration directory must exist before you can continue this installation.
18. The setup program then asks if you want to use a different installation for your user directory. The default is `no` (this installation will be the user directory). However, if you intend this server instance to be used as a configuration directory only, then you should enter **`yes`**.
19. For the Directory Server port, select the default; this will be 389 or a randomly-generated port number if you already have another application using that port or you are not installing as root.
20. For the Directory Server Identifier, enter a unique value (normally the default is sufficient).

    This value is used as part of the name of the directory in which the Directory Server instance is installed. For example, if your machine's host name is `phonebook`, then this name is the default, and selecting it will cause the Directory Server instance to be installed into a directory labeled `slapd-phonebook`.

Caution

The Directory Server identifier must not contain a period. For example, example.server.com is not a valid server identifier name.

21. For configuration directory administrator ID and password, enter the name and password as whom you will log in when you want to authenticate to the **Console** with full privileges.
22. For a directory suffix, enter a *distinguished name* (DN) meaningful to your enterprise.

    This string is used to form the name of all your organization's directory entries. Therefore, pick a name that is representative of your organization. It is recommended that you pick a suffix that corresponds to your Internet DNS name. Avoid space characters in the suffix.

    For example, if your organization uses the DNS name `example.com`, then enter `dc=example,dc=com` here.
23. For Directory Manager DN, enter the DN that you will use when managing the contents of your directory with unlimited privileges.

Note

Any DN must be entered in the UTF-8 character set encoding. Older encodings such as ISO-8859-1 are not supported.

    In former releases of Directory Server, the Directory Manager was known as the *root DN*. This is the entry that you use to bind to the directory when you want access control to be ignored. This DN can be short and does not have to conform to any suffix configured for your directory. However, it should not correspond to an actual entry stored in your directory.

    For the Directory Manager password, enter a value that is at least 8 characters long.
24. For Administration Domain, enter the domain to which you want this server to belong.

    The name you enter should be a unique string that is descriptive of the organization responsible for administering the domain. For information on administration domains, refer to Section 1.2.8 *Determining the Administration Domain*.
25. For the administration port number, enter a value that is not in use (an available port number is randomly generated as the default). Be sure to record this value.
26. For the user as whom you want to run Administration Server, enter root. This is the default. You have to run this as root if your port number is below 1024; otherwise, you can run this as a regular user.

    The server is then unpackaged, minimally configured, and started. You are told on what host and port number Administration Server is listening.

    The server is configured to use the following suffixes:

    - The suffix that you configured.
    - o=NetscapeRoot

    Do not modify the contents of the directory under the `o=NetscapeRoot` suffix. Either create data under the first suffix or create a new suffix to be used for this purpose. For details on how to create new suffixes for your Directory Server, see the *Red Hat Directory Server Administration Guide*.

3.3. Installing on Red Hat Enterprise Linux using an Express Installation

1. Log in as root.
2. If you have not already done so, download the product binaries file to the installation directory.
3. Use the rpm tool to install the server components, as follows:
   ```
   rpm -ivh package.rpm
   ```
   The server components are then installed in the default location: `/opt/redhat-ds/`.
4. Next, you need to create an instance of the Directory Server by running the setup program:
   ```
   cd /opt/redhat-ds/
   ./setup/setup
   ```
5. Type **y** to accept the licensing agreement, then **y** again to continue with setup.
6. Type **y** to continue with setup once dsktune has completed. Refer to Section 2.3.1 *dsktune Utility* for more information.
7. Select the installation mode (express installation).
8. For the hostname, either enter a fully qualified hostname or select the default (which is the local host).

   Caution

   The default hostname may be incorrect if the installer cannot locate a DNS name in your system. For example, you might not have a DNS name if your system uses NIS.

   The hostname must be a fully qualified host and domain name. If the default hostname is not a fully qualified host and domain name, installation will fail. Refer to Section 7.2 *Common Installation Problems* for more information about entering a fully qualified domain name.
9. The setup program then asks you for the *System User* and the *System Group* names. Enter the identity under which you want the servers to run.

   For more information on the user and group names that you should use when running your servers, refer to Section 1.2.3 *Deciding the User and Group for Your Servers*.
10. For the configuration directory administrator ID and password, enter the name and password as whom you will log in when you want to authenticate to the **Console** with full privileges.
11. For the Directory Manager DN, enter the DN that you will use when managing the contents of your directory with unlimited privileges.

    Note

    Any DN must be entered in the UTF-8 character set encoding. Older encodings such as ISO-8859-1 are not supported.

    In former releases of Directory Server, the Directory Manager was known as the *root DN*. This is the entry that you use to bind to the directory when you want access control to be ignored. This DN can be short and does not have to conform to any suffix configured for your directory. However, it should not correspond to an actual entry stored in your directory.

    For the Directory Manager password, enter a value that is at least 8 characters long.

3.4. Installing on Red Hat Enterprise Linux Using a Typical Installation

To install Directory Server on Red Hat Enterprise Linux, do the following:

1. Log in as root.
2. If you have not already done so, download the product binaries file to the installation directory.
3. Use the rpm tool to install the server components, as follows:
   `rpm -ivh package.rpm`

   The server components are then installed in the default location: `/opt/redhat-ds/`.
4. Next, you need to create an instance of the Directory Server by running the setup program:
   ```
   cd /opt/redhat-ds/
   ./setup/setup
   ```
5. Type **y** to accept the licensing agreement, then **y** again to continue with setup.
6. Select the installation mode; the default is typical installation.
7. For the hostname, either enter a fully qualified hostname or select the default (which is the local host).

   Caution

   The default hostname may be incorrect if the installer cannot locate a DNS name in your system. For example, you might not have a DNS name if your system uses NIS.

   The hostname must be a fully qualified host and domain name. If the default hostname is not a fully qualified host and domain name, installation fails. Refer to Section 7.2 *Common Installation Problems* for more information about entering a fully qualified domain name.
8. The setup program then asks you for the *System User* and the *System Group* names. Enter the identity under which you want the servers to run.

   For more information on the user and group names that you should use when running your servers, refer to Section 1.2.3 *Deciding the User and Group for Your Servers*.
9. For the configuration directory, select the default if this directory will host your `o=NetscapeRoot` tree. Otherwise, enter yes. You will then be asked for the contact information for the configuration directory.

   If the server you are currently installing is not the configuration directory, then the configuration directory must exist before you can continue this installation.
10. The setup program then asks if you want to use a different installation for your user directory. The default is `no` (this installation will be the user directory). However, if you intend this server instance to be used as a configuration directory only, then you should enter **yes**.
11. For the Directory Server port, select the default; this will be 389 or a randomly-generated port number if you already have another application using that port or you are not installing as root.
12. For the Directory Server Identifier, enter a unique value (normally the default is sufficient).

    This value is used as part of the name of the directory in which the Directory Server instance is installed. For example, if your machine's host name is phonebook, then this name is the default, and selecting it will cause the Directory Server instance to be installed into a directory labeled `slapd-phonebook`.

Caution

The Directory Server identifier must not contain a period. For example, example.server.com is not a valid server identifier name.

13. For the configuration directory administrator ID and password, enter the name and password as whom you will log in when you want to authenticate to the **Console** with full privileges.
14. For a directory suffix, enter a distinguished name (DN) meaningful to your enterprise.

    This string is used to form the name of all your organization's directory entries. Therefore, pick a name that is representative of your organization. It is recommended that you pick a suffix that corresponds to your Internet DNS name. Avoid space characters in the suffix.

    For example, if your organization uses the DNS name `example.com`, then enter `dc=example,dc=com` here.
15. For the Directory Manager DN, enter the DN that you will use when managing the contents of your directory with unlimited privileges.

Note

Any DN must be entered in the UTF-8 character set encoding. Older encodings such as ISO-8859-1 are not supported.

    In former releases of Directory Server, the Directory Manager was known as the *root DN*. This is the entry that you use to bind to the directory when you want access control to be ignored. This DN can be short and does not have to conform to any suffix configured for your directory. However, it should not correspond to an actual entry stored in your directory.

    For the Directory Manager password, enter a value that is at least 8 characters long.
16. For Administration Domain, enter the domain to which you want this server to belong.

    The name you enter should be a unique string that is descriptive of the organization responsible for administering the domain. For information on administration domains, refer to Section 1.2.8 *Determining the Administration Domain*.
17. For the administration port number, enter a value that is not in use (an available port number will be randomly generated as the default). Be sure to record this value.
18. For the user as whom you want to run Administration Server, enter root. This is the default. You have to run this as root if your port number is below 1024; otherwise, you can run this as a regular user.

    The server is then unpackaged, minimally configured, and started. You are told on what host and port number Administration Server is listening.

    The server is configured to use the following suffixes:

    - The suffix that you configured.
    - `o=NetscapeRoot`

    Do not modify the contents of the directory under the `o=NetscapeRoot` suffix. Either create data under the first suffix or create a new suffix to be used for this purpose. For details on how to create new suffixes for your Directory Server, see the *Red Hat Directory Server Administration Guide*.

Chapter 4.
Silent Installation and Instance Creation

Silent installation allows you to use a file to predefine all the answers that you would normally supply to the setup program interactively; this provides you with the ability to script the installation of multiple instances of Red Hat Directory Server (Directory Server). Instance creation enables you to use an existing Directory Server instance to create additional instances of the server under the same server root.

This chapter explains the following:

- Section 4.1 *Using Silent Installation*
- Section 4.2 *Using Silent Instance Creation*.

4.1. Using Silent Installation

Silent installation is intended for use at sites where many server instances must be created. For Directory Server, it is especially useful for heavily replicated sites that create a large number of replica servers.

To use silent installation, you create a silent installation file, supply values for the appropriate installation directives, and run the setup program with the -s and -f command-line options.

The procedure below explains how to use silent installation:

1. Log in as root.
2. Create a new directory:
   ```
   mkdir ds
   cd ds
   ```
3. If you have not already done so, download the product binaries file to the installation directory.
4. Unpack the product binaries file using the following command:
   ```
   gunzip -dc filename.tar.gz | tar -xvof-
   ```
   where *filename* corresponds to the product binaries file that you want to unpack.
5. Prepare the file that contains your installation directives.

   Refer to Section 4.1.2 *Preparing Silent Installation Files* for instructions and for some examples of the silent-install files.
6. Fill in appropriate values for the installation directives.

   Refer to Section 4.1.3 *Specifying Silent Installation Directives* for the complete list of silent installation directives that you can use when installing Directory Server.
7. Run the setup program with the `-s` and `-f` command-line options:
   ```
   setup -s -f filename
   ```
   where *filename* is the name of the file that contains your installation directives.

4.1.1. Silent Installation on Red Hat Enterprise Linux

It is possible to use silent instance creation on Red Hat Enterprise Linux servers.

1. Log in as root.
2. Create a new directory:
   ```
   mkdir ds
   cd ds
   ```
3. If you have not already done so, download the product binaries file to the installation directory.
4. Install the Directory Server as normal, using the command line or the Red Hat RPM tool, **system-config-packages** (refer to Section 3.4 *Installing on Red Hat Enterprise Linux Using a Typical Installation*).
5. Prepare the file that contains your installation directives.

   Refer to Section 4.1.2 *Preparing Silent Installation Files* for instructions and for some examples of the silent-install files.
6. Fill in appropriate values for the installation directives.

   Refer to Section 4.1.3 *Specifying Silent Installation Directives* for the complete list of silent installation directives that you can use when installing Directory Server.
7. When you run the setup program, specify the .inf file you have created, as follows:
   ```
   /opt/redhat-ds/servers/setup/silent.inf
   ```

4.1.2. Preparing Silent Installation Files

The best way to create a file for use with silent installation is to use the setup program to create interactively a server instance of the type that you want to duplicate. To do this, run setup with the -k flag. The setup program creates the following file:

```
serverRoot/setup/install.inf
```

This file contains all the directives that you would use with silent installation to create the server instance. You can then use this file to create other server instances of that type.

You have to make some modifications to this file before you use it. Specifically, ensure that you have done the following:

- *FullMachineName* - Set this directive to a value that is appropriate for the machine on which Directory Server is installed if it is not to be the local machine. In most circumstances, it is best not to use this directive because *FullMachineName* then defaults to the local host name. However, if you use custom installation to generate your initial server instance, then this directive appears in the `install.inf` file.
- *ServerIpAddress* - Set this directive appropriate for the local machine. The same usage rules apply for *ServerIpAddress* as for *FullMachineName*. Specifically, try not to include *ServerIpAddress* in your install.inf file unless you absolutely have to (as may be necessary for multi-homed systems).
- *ServerRoot* - Verify the installation path on this directive. Also, the name of the file-system directory where you install files must not contain any space characters.
- *ServerIdentifier* - If you are installing more than one Directory Server on the same host, make sure that this directive contains a unique value for each server instance.

- *SuiteSpotUserID* and SuiteSpotGroup - The *SuiteSpotUserID* and *SuiteSpotGroup* directives determine under what user and group a server runs when installed.

Note

Be sure to protect your install.inf files because they contain passwords in clear. Also ensure that any DNs in these files are in the UTF-8 character set encoding.

The sections that follow provide examples of using silent installation to support the following installation scenarios:

- Section 4.1.2.1 *Sample File for Typical Installation*
- Section 4.1.2.2 *Sample File for Using an Existing Configuration Directory*
- Section 4.1.2.3 *Sample File for Installing the Standalone Red Hat Console*.

You can find a definition of each of the individual installation directives in Section 4.1.3 *Specifying Silent Installation Directives*.

Note

The `silent.inf` file provided with the Directory Server is merely a template, an example of how to write your own. For the file to work, many of the parameters (host name, ports, paths, and so on) in the file must be replaced with appropriate values.

It is also easy to generate your own silent installation file using the setup `-k` option and modifying the resulting `install.inf` file as needed.

4.1.2.1. Sample File for Typical Installation

The following is an example of the `install.inf` file that is generated for a typical installation:

```
[General]
FullMachineName= dir.example.com
SuiteSpotUserID= nobody
SuiteSpotGroup= nobody
ServerRoot= /opt/redhat-ds/servers
AdminDomain= example.com
ConfigDirectoryAdminID= admin
ConfigDirectoryAdminPwd= admin
ConfigDirectoryLdapURL= ldap://dir.example.com:389/o=NetscapeRoot
UserDirectoryAdminID= admin
UserDirectoryAdminPwd= admin
UserDirectoryLdapURL= ldap://dir.example.com:389/dc=example,dc=com
Components= svrcore,base,slapd,admin,nsperl,perldap

[slapd]
SlapdConfigForMC= Yes
SecurityOn= No
UseExistingMC= No
UseExistingUG= No
ServerPort= 389
ServerIdentifier= dir
Suffix= dc=example,dc=com
```

```
RootDN= cn=Directory Manager
UseReplication= No
AddSampleEntries= No
InstallLdifFile= suggest
AddOrgEntries= Yes
DisableSchemaChecking= No
RootDNPwd= admin123
Components= slapd,slapd-client

[admin]
SysUser= root
Port= 23611
ServerIpAddress= 111.11.11.11
ServerAdminID= admin
ServerAdminPwd= admin
Components= admin,admin-client

[base]
Components= base,base-client,base-jre

[nsperl]
Components= nsperl561

[perldap]
Components= perldap14
```

4.1.2.2. Sample File for Using an Existing Configuration Directory

The following is an example of the `install.inf` file that is generated when you perform a typical installation and you choose to use an existing Directory Server as the configuration directory:

```
[General]
FullMachineName= dir.example.com
SuiteSpotUserID= nobody
SuiteSpotGroup= nobody
ServerRoot= /opt/redhat-ds/servers
AdminDomain= example.com
ConfigDirectoryAdminID= admin
ConfigDirectoryAdminPwd= admin
ConfigDirectoryLdapURL= ldap://dir.example.com:25389/o=NetscapeRoot
UserDirectoryLdapURL= ldap://dir.example.com:18257/dc=example,dc=com
UserDirectoryAdminID= cn=Directory Manager
UserDirectoryAdminPwd= admin123
Components= svrcore,base,slapd,admin,nsperl,perldap

[slapd]
SlapdConfigForMC= No
SecurityOn= No
UseExistingMC= Yes
UseExistingUG= No
ServerPort= 18257
ServerIdentifier= directory
Suffix= dc=example,dc=com
RootDN= cn=Directory Manager
UseReplication= No
AddSampleEntries= No
InstallLdifFile= suggest
AddOrgEntries= Yes
DisableSchemaChecking= No
RootDNPwd= admin123
```

```
Components= slapd,slapd-client

[admin]
SysUser= root
Port= 33646
ServerIpAddress= 111.11.11.11
ServerAdminID= admin
ServerAdminPwd= admin
Components= admin,admin-client

[base]
Components= base,base-client,base-jre

[nsperl]
Components= nsperl561

[perldap]
Components= perldap14
```

4.1.2.3. Sample File for Installing the Standalone Red Hat Console

The following is an example of the install.inf file that is generated when you install just Red Hat Console:

```
[General]
FullMachineName= dir.example.com
ConfigDirectoryLdapURL= ldap://dir.example.com:389/o=NetscapeRoot
SuiteSpotUserID= nobody
SuiteSpotGroup= nobody
ConfigDirectoryAdminID= admin
ConfigDirectoryAdminPwd= admin
ServerRoot= /opt/redhat-ds/servers
Components= svrcore,base,slapd,admin

[base]
Components= base-client

[slapd]
Components= slapd-client

[admin]
Components= admin-client,base-jre
```

4.1.3. Specifying Silent Installation Directives

This section describes the basic format of the file used for silent installation. It then describes the directives that are available for each area of the silent installation file.

- Section 4.1.3.1 *Silent Installation File Format*
- Section 4.1.3.2 *`[General]` Installation Directives*
- Section 4.1.3.3 *`[slapd]` Installation Directives*
- Section 4.1.3.4 *[admin] Installation Directives*
- Section 4.1.3.5 *[Base] Installation Directive*

- Section 4.1.3.6 *[nsperl] Installation Directives*
- Section 4.1.3.7 *[perldap] Installation Directives*.

4.1.3.1. Silent Installation File Format

When you use silent installation, you provide all the installation information in a file. This file is formatted as follows:

```
[General]
directive=value
directive=value
directive=value
...

[slapd]
directive=value
directive=value
directive=value
...

[admin]
directive=value
directive=value
directive=value
...

[Base]
directive=value
directive=value
directive=value
...
```

The keywords `[General]`, `[slapd]`, and `[admin]` are required. They indicate that the directives that follow are meant for a specific aspect of the installation. They must be provided in the file in the order indicated above.

4.1.3.2. `[General]` Installation Directives

`[General]` installation directives specify information of global interest to the Directory Servers installed at your site. That is, the information you provide here is common to all your Directory Servers.

The *[General]* installation directives are listed in Table 4-1.

Directive	Description

Directive	Description
Components	Specifies components to be installed. The list of available components differs depending on the servers available on your installation media. For stand-alone directory installation, the list of components is: *svrcore* - Uninstallation binaries *base* - The base installation package *admin* - The Administration Server binaries *slapd* - The Directory Server binaries This directive is required. At a minimum, you should always provide *components=svrcore,base,admin*
ServerRoot	Specifies the full path to the directory where the Directory Server binaries are installed. This directive is required.
FullMachineName	Specifies the fully qualified domain name of the machine on which you are installing the server. The default is the local host name.
SuiteSpotUserID	Specifies the user name the servers run as. This parameter does not apply to the user as which the Administration Server runs. See the *SysUser* directive in Table 4-4 for more information. The default is user *nobody*, but this should be changed for most deployments.
SuiteSpotGroup	Specifies the group the servers run as. The default is group nobody, but this should be changed for most deployments.
ConfigDirectoryLdapURL	Specifies the LDAP URL that is used to connect to your configuration directory. LDAP URLs are described in the *Red Hat Directory Server Administration Guide*. This directive is required.
AdminDomain	Specifies the administration domain that this server is registered under. Refer to Section 1.2.8 *Determining the Administration Domain* for more information about administration domains.
ConfigDirectoryAdminID	Specifies the user ID of the entry that has administration privileges to the configuration directory. This directive is required.
ConfigDirectoryAdminPwd	Specifies the password for the *ConfigDirectoryAdminID*. This directive is required.
UserDirectoryLdapURL	Specifies the LDAP URL that is used to connect to the directory where your user and group data are stored. If this directive is not supplied, the configuration directory is used for this purpose. LDAP URLs are described in the ^*Red Hat Directory Server Administration Guide*.
UserDirectoryAdminID	Specifies the user ID of the entry that has administration privileges to the user directory.
UserDirectoryAdminPwd	Specifies the password for the *UserDirectoryAdminID*.

Table 4-1. `[General]` Installation Directives

4.1.3.3. `[slapd]` Installation Directives

`[slapd]` installation directives specify information of interest only to the Directory Server instance that you are currently installing. These directives are classified as follows:

Required `[slapd]` Installation Directives

You must provide these directives when you use silent installation with Directory Server.

Optional `[slapd]` Installation Directives

You may provide these directives when you use silent installation with Directory Server.

Table 4-2 and Table 4-3 list the directives.

Required Directive	Description
Components	Specifies the `slapd` components to be installed. The components are: slapd - Install Directory Server slapd-client - Install Directory Server **Console** This directive is required. It is recommended that you always install both components any time you install the Directory Server.
ServerPort	Specifies the port the server uses for LDAP connections. For information on selecting server port numbers, see Section 1.2.1 *Choosing Unique Port Numbers*. This directive is required.
ServerIdentifier	Specifies the server identifier. This directive is required. This value is used as part of the name of the directory in which the Directory Server instance is installed. For example, if your machine's host name is phonebook, then this name is the default, and selecting it causes the Directory Server instance to be installed into a directory labeled `slapd-phonebook`.
Suffix	Specifies the suffix that you store your directory data under. For information on suffixes, see Section 1.2.5 *Determining Your Directory Suffix*. This directive is required.
RootDN	Specifies the distinguished name used by the directory manager. For information on the directory manager, see Section 1.2.4 *Defining Authentication Entities*. This directive is required.
RootDNPwd	Specifies the directory manager's password. This directive is required.

Table 4-2. Required `[slapd]` Installation Directives

Optional Directive	Description
AddSampleEntries	If set to yes, this directive causes the example.ldif sample directory to be loaded. Use this directive if you are installing the Directory Server for evaluation purposes and you do not already have an LDIF file with which to populate your directory. Default is no.
AddOrgEntries	If set to yes, this directive causes the new Directory Server instance to be created with a suggested directory structure and access control. If this directive is used and InstallLdifFile is also used, then this directive has no effect. Default is *no*.

Optional Directive	Description
InstallLdifFile	Causes the contents of the LDIF file to be used to populate your directory.

Table 4-3. Optional [slapd] Installation Directives

4.1.3.4. [admin] Installation Directives

[admin] installation directives specify information of interest only to your Directory Server's Administration Server. That is, this is the installation information required for the Administration Server that is used to manage the Directory Server instance that you are currently installing.

The [admin] installation directives are listed in Table 4-4.

Directive	Description
Components	Specifies the admin components to be installed. The base components are: *admin* - Install Administration Server. You must install the Administration Server if you are also installing some other server, such as Directory Server *admin-client* - Install **Red Hat Console** Specify just this component if you are installing **Red Hat Console** as stand-alone. Do not install this component if you do remotely manage your servers and **Red Hat Console** is installed somewhere else on your network.
SysUser	Specifies the user the Administration Server runs as. For default installations that use the default port numbers, this user must be root, which is the default. For information as to what users your servers should run, refer to Section 1.2.3 *Deciding the User and Group for Your Servers*.
Port	Specifies the port that the Administration Server uses. The Administration Server's host name is given by the *FullMachineName* directive. For more information on *FullMachineName*, refer to Table 4-1.
ServerAdminID	Specifies the administration ID that can be used to access this Administration Server if the configuration directory is not responding. The default is to use the value specified by the ConfigDirectoryAdminID directive. See Section 1.2.4 *Defining Authentication Entities* for information on this directive.
ServerAdminPwd	Specifies the password for ServerAdminID.
ServerIpAddress	Specifies the IP address the Administration Server listens to. Use this directive if you are installing on a multi-homed system and you do not want to use the first IP address for your Administration Server.

Table 4-4. [admin] Installation Directives

4.1.3.5. [Base] Installation Directive

There is only one [Base] installation directive, and it allows you to determine whether Red Hat Console is installed. Table 4-5 the directive.

Directive	Description
Components	Specifies the base components to be installed. The base components are: *base* - Install the shared libraries used by all Server Consoles. You must install this package if you are also installing some other server, such as Directory Server. *base-client* - Install the Java run time environment used by the Server Consoles. *base-jre* - Causes the Java run time environment to be installed. This directive is required if you are installing a server instead of just the Console. You must install both packages when you are installing a server.

Table 4-5. [Base] Installation Directive

4.1.3.6. [nsperl] Installation Directives

There is only one [nsperl] installation directive, and it allows you to determine whether nsPerl is to be installed. Table 4-6 lists the directive.

Directive	Description
Components	Specifies whether nsperl that is bundled with Directory Server is to be installed. This nsPerl is a CPAN perl, built and maintained for use by Red Hat server products. The *nsperl561* (Install nsPerl version 5.6.1.) directive is required if you are installing a server instead of just the **Console**.

Table 4-6. [nsperl] Installation Directive

4.1.3.7. [perldap] Installation Directives

There is only one *[perldap]* installation directive, and it allows you to determine whether PerLDAP is to be installed. Table 4-7 lists the directive.

Directive	Description
Components	*perldap14* - Install perLDAP version 1.4.1. specifies whether perldap that is bundled with Directory Server is to be installed. This is mozilla.org PerLDAP, built and maintained at Red Hat and used by Red Hat server products. This directive is required if you are installing a server instead of just the **Console**.

Table 4-7. [perldap] Installation Directive

4.2. Using Silent Instance Creation

If you have Directory Server installed in a server root, you can create additional instances of Directory Server under the same server root without having to run the setup program. You can create additional instances of the server either by using **Red Hat Console** or from the command-line.

Because all instances of Directory Server under a server root use the same Administration Server, the instance creation process does not install Administration Server binaries; you cannot create two instances of Administration Server in one server root.

Having multiple instances in a single server root is useful for testing and for when one host is used for multiple purposes. Keep in mind that each Directory Server instance must be assigned a different port number and server identifier.

The `ds_create` program, which is located in the *`serverRoot`*`/bin/slapd/admin/bin` directory, enables you to create additional instances of Directory Server under a server root. You may want to use this program when you already have Directory Server installed and just want to create additional instances of the server from the commandline.

To create a new instance of Directory Server, run this command from the *`ServerRoot`*`/bin/slapd/admin/bin` directory:

```
ds_create -f filename
```

Where *`filename`* is the silent instance creation file, which must be similar to the file used with the setup program (refer to Section 4.1.2 *Preparing Silent Installation Files*) except that the file must only contain the following two sections:

- `[General]`
- `[slapd]`

These sections do not take the `Components` directive.

Here's a sample file for instance creation. The `\` is inserted to break the line for printing purposes. You need to remove the `\` and make that one single line.

```
[General]
FullMachineName= testDir.example.com
ServerRoot= /opt/redhat-ds/servers
AdminDomain= example.com
ConfigDirectoryAdminID= admin
ConfigDirectoryAdminPwd= secretPwd01
ConfigDirectoryLdapURL= ldap://testDir.example.com:389/o=NetscapeRoot
UserDirectoryAdminID= admin
UserDirectoryAdminPwd= secretPwd02
UserDirectoryLdapURL= ldap://testDir.example.com:389/dc=europe,dc=example,\
dc=com

[slapd]
ServerPort= 389
ServerIdentifier= instance02
RootDN= cn=Directory Manager
RootDNPwd= DirMgrPwd
Suffix= dc=europe,dc=example,dc=com
SlapdConfigForMC= No
UseExistingMC= Yes
UseExistingUG= No
SecurityOn= No
UseReplication= No
AddSampleEntries= No
InstallLdifFile= suggest
AddOrgEntries= Yes
```

```
DisableSchemaChecking= No
```

Chapter 5.

Post Installation

This chapter describes the post-installation procedures for launching the online help and populating the directory tree.

This chapter has the following sections:

- Section 5.1 *Launching the Help System*
- Section 5.2 *Populating the Directory Tree*

5.1. Launching the Help System

The help system for Directory Server is dependent upon **Red Hat Administration Server**. If you are running **Directory Server Console** on a machine remote to Administration Server, you will need to confirm authorizations on Administration Server.

Client IP address authorized on Administration Server

The machine running Directory Server Console needs access to Administration Server. Configure Administration Server to accept the client machine's IP address in Administration Server:

1. Launch **Administration Server Console**. The **Console** should be running on the same machine as Administration Server.
2. Click the **Configuration** tab, then click the **Network** tab.
3. In the **Connection Restrictions Settings**, select **IP Addresses to Allow** from the pull down menu. Click **Edit**.
4. Change the IP Addresses field to the following: `*.*.*.*`

   This allows all clients access to Administration Server.
5. Restart Administration Server. You can now launch the online help by clicking any of the **Help** buttons in the **Directory Server Console**.

Proxy authorized on Administration Server

If you use proxies for your HTTP connections on the client machine running **Directory Server Console**, you need to do one of the following:

- Remove proxies on the machine running **Directory Server Console**. This allows the client machine to access Administration Server directly.

  To remove the proxies on the machine running **Directory Server Console**, you need to alter the proxy configuration of the browser you will use to run the help.
- Add the client machine proxy IP address to Administration Server list of acceptable IP addresses.

Caution

Adding the client machine proxy IP address to Administration Server creates a potential security hole in your system.

5.2. Populating the Directory Tree

During installation, a simple directory database was created for you. In addition, a simple directory structure was placed in the database for you to use. This directory structure contained basic access control and the major branch points for the recommended directory structure.

Now you need to populate your database with user entries. There are several ways you can create and populate your directory suffixes. These are explained in detail in the *Red Hat Directory Server Administration Guide*.

The main methods are:

- Create a database from LDIF: Use this method if you want to use the sample directory data shipped with Directory Server, if you are importing entries from another directory via LDIF, or if you have more than a few entries to add at once. For more information about LDIF, refer to the *Red Hat Directory Server Administration Guide*.
- Start your Directory Server with an empty database and import data over LDAP: This method requires you to populate your directory using an LDAP client such as Directory Server **Gateway** or the `ldapmodify` command-line utility. Use this method if you have just a few entries to add at a time. For information on setting up the Directory Server **Gateway**, refer to the *Red Hat Directory Server Gateway Customization Guide*. This document is provided with *Red Hat Directory Server Resource Kit*.

As you are populating your directory, consider your access control needs and set access control accordingly. For more information on access control, see the *Red Hat Directory Server Deployment Guide* and the *Red Hat Directory Server Administration Guide*.

Chapter 6.

Migrating from Previous Versions

If you have a previous installation of Directory Server, depending on its version, you can migrate to Red Hat Directory Server 7.x. *Migration* refers to the process of moving Directory Server 6.x files to Directory Server 7.x.

This chapter covers the migration process in these sections:

- Section 6.1 *Migration Overview*
- Section 6.2 *Migration Prerequisites*
- Section 6.3 *Migration Procedure*
- Section 6.4 *Upgrading from Directory Server 7.x Versions*.

6.1. Migration Overview

You can migrate Directory Server 6.2, 6.21, and 7.0; versions 6.11 and before cannot be migrated or upgraded to Directory Server 7.1. For these releases, as well as migrating from SunOne Directory Server, it is recommended that you export the databases to LDIF, install a fresh Directory Server, and import the LDIF data.

Before you migrate your directory service, you should become familiar with the new features offered in 7.1 release of the Directory Server.

The migration process is performed by running the `migrateInstance7` script on the system where your Directory Server is installed. You must shut down your directory service before running the migration script; if you do not, the script shuts down the server.

The migration script performs the following tasks in sequence:

- Checks the schema configuration files and notifies you of any changes between the standard configuration files and the ones present on your system.
- Creates a database for each suffix stored in the legacy Directory Server. (In current releases of Directory Server, you can have multiple databases but just one suffix per database.)
- Checks if any database exists and, if it does, gives you the option to save the database (by exporting it to a file), skip the database, or overwrite the database.
- Migrates the server parameters and database parameters. (These are stored as LDAP entries in the `dse.ldif` file.)
- Migrates user-defined schema objects.
- Migrates indexes.
- Migrates standard server plug-ins.
- Migrates the certificate database and SSL parameters.
- Migrates database links.
- Migrates replication entries (changelog).
- Migrates the SNMP configuration.

The migration script shuts down your legacy Directory Server before performing the migration process. The migration script also backs up your current configuration.

6.2. Migration Prerequisites

This section lists the prerequisites that your system must meet before you can consider beginning the migration process.

- You must be using Directory Server 6.x. When you run the migration script, the legacy server process `ns-slapd` should be stopped. (If you do not stop the server, the migration script stops it.)
- Your legacy Directory Server and your new Directory Server must be installed on the same host; migration cannot occur over networked drives.
- Do not install the new Directory Server on top of an existing Directory Server installation. Install your new Directory Server in a separate directory. Migrate your legacy directory data into your new directory, and, when you are satisfied with the result of the migration, remove your legacy Directory Server.
- If you want to continue to run your legacy Directory Server, choose different ports for LDAP traffic and for secured connections than the ones used by your legacy Directory Server when you install the new Directory Server.

  If you are not going to run your legacy Directory Server, use the same port numbers to ensure that any directory clients that have static configuration information (including Directory Server port numbers) continue to work.
- Your new Directory Server must be running when you execute the migration script.
- Any custom schema that you created in a 6.x Directory Server must be stored in an LDIF file in the *serverRoot*`/slapd-`*serverID*`/config/schema` directory.
- Before performing the migration, check that the user-defined variables contain the following associated values, where *server7Root* is the path to where your new Directory Server 7.x is installed:

  Set the following environment variables:
  `PERL5LIB=`*server7Root*`/bin/slapd/admin/bin`
  `PATH=`*server7Root*`/bin/slapd/admin/bin:$PATH`
- When you run the migration script, it migrates the configuration files or configuration entries, database instances, and schema with minimum manual intervention. For complete information on the configuration parameters and attributes that are migrated, refer to the section on migrating from earlier versions in the *Red Hat Directory Server Configuration, Command, and File Reference*.
- Check the command syntax for the migration script in the section on command-line scripts of the *Red Hat Directory Server Configuration, Command, and File Reference*.

6.3. Migration Procedure

Before you start with migration process, ensure the following:

- Read sections Section 6.1 *Migration Overview* and Section 6.2 *Migration Prerequisites*.
- The migration script will automatically back up your Directory Server configuration if it is in the default location.
  - If you are migrating from Directory Server 6.x, all of the configuration files in the `/opt/redhat-ds/servers/slapd-`*serverID*`/config` directory will be backed up to a directory named *serverRoot*`/slapd-`*serverID*`/config_backup`.
  - If your configuration files are stored in non-default locations, before you migrate your server, copy them to a secure place.

This section contains the following information:

- Section 6.3.1 *Migrating a Standalone Server*
- Section 6.3.2 *Migrating a 6.x Replicated Site*
- Section 6.3.3 *Migrating a 6.x Multi-Master Deployment*
- Section 6.3.4 *Managing Console Failover*.

6.3.1. Migrating a Standalone Server

Once you have backed up your critical configuration information, do the following to migrate a server:

1. Stop your legacy Directory Server.

   If you do not stop the legacy Directory Server, the migration script does it for you.

2. On the machine where your legacy Directory Server is installed, install a new 7.x Directory Server. This installation process is described in Chapter 3 *Using Express and Typical Installation* or Chapter 4 *Silent Installation and Instance Creation*.

   Use the same port numbers as your legacy production server if you want to ensure that any directory clients that have static configuration information (including Directory Server port numbers) continue to work.

3. Run the migration script.

   As root user, change directory to *serverRoot*/bin/slapd/admin/bin. Then enter the following command:

   ```
   migrateInstance7 -D rootDN -w password -p port
       -o oldInstancePath -n newInstancePath
   ```

   Where:

   - *rootDN* is the Directory Server 7.x user DN with root permissions, such as Directory Manager.
   - *password* is the password for Directory Manager in Directory Server 7.x.
   - *port* is the LDAP port number assigned to Directory Server 7.x.
   - *oldInstancePath* is the path to the installation directory of the legacy Directory Server (for example, /opt/redhat-ds/server6/slapd-*serverID*).
   - *newInstancePath* is the path to the installation directory of Directory Server 7.x (for example, /opt/redhat-ds/servers/slapd-*serverID*).

   The following is an example of a command you would use to migrate an instance of Directory Server 6.21 to Directory Server 7.1:

   ```
   migrateInstance7 -D cn=Directory Manager -w secret -p 389 \
      -o /opt/redhat-ds/server621/slapd-phonebook \
      -n /opt/redhat-ds/servers/slapd-phonebook \
   ```

   This command appears on one line in usage. The slashes \ are used to wrap the line for printing, and should be removed when using the command.

4. Follow the prompts. For example, if you're prompted to provide a path and filename for your backup directory, enter one or accept the default.

The migration process starts. At the end of migration, your legacy Directory Server is migrated. Additionally, as a result of this migration, a new Directory Server 7.x instance is installed using the configuration information obtained from your legacy Directory Server; the data from your old server is migrated to the new server; and the new server is started.

A sample output in Example 6-1 shows a migration of Directory Server 6.21 to Directory Server 7.1. The migration script detects three backends, backend1, backend2, and userRoot, which exist in

the legacy server as well as in the new server instances. To demonstrate the various options, for each backend a different option was chosen: for `backend1`, the choice was to continue with the migration and export processes; for `backend2`, the choice was to continue with the migration process only, without exporting; and, for `userRoot`, the choice was to skip the migration process.

In this sample, the \ has been inserted to indicate a line break for printing purposes.

```
migrateInstance7 -D "cn=directory manager" -w password -p 389 -o
/export/server621/slapd-marmot -n /export/server71/slapd-marmot

******* Migration from 6.21 to 7.1 Directory Server *********

Shutdown the legacy Directory Server instance: /export/server621/\
slapd-marmot

Shutting down server slapd-marmot . . .

. . . . . .

Backup /export/server71/slapd-marmot/config on
/export/server71/slapd-marmot/config_backup ...

Where do you want to back up your configuration directory
[/export/server71/slapd-marmot/config_backup] ?

Migrate the schema...

Shutting down server slapd-marmot . . .

. . . . . .

*****************************************************************

The following LDIF files have been migrated:

99user.ldif

*****************************************************************


-----------------------------------------------------------------


Migrate key/cert databases...

Shutting down server slapd-marmot . . .

. . .


/export/server71/alias/slapd-marmot-key3.db already exists. Do
you want to overwrite it ? [no]: y

/export/server71/alias/slapd-marmot-cert8.db already exists. Do
you want to overwrite it ? [no]: y


Connected to 7.1 LDAP server

-----------------------------------------------------------------
```

```
Parse the old DSE ldif file: /export/server621/slapd-marmot/
config/dse.ldif

*****

This may take a while ...


Migrate DSE entries...

SECURITY - Update successfull: cn=encryption,cn=config

SNMP - Update successfull: cn=snmp,cn=config

------------------------------------------------------------------

Migrate LDBM backend instances...


*** LDBM_BACKEND_INSTANCE - cn=backend1,cn=ldbm database,\
cn=plugins,cn=config

already exists

*** Migration will overwrite existing database

Do you want to continue Yes/No [No] ? y

Do you want to export the existing data Yes/No [Yes] ? y


Enter the full pathname of the file

[/export/server71/slapd-marmot/db_backup/backend1.ldif]:


Existing data will be exported under

/export/server71/slapd-marmot/db_backup/backend1.ldif

Continue Yes/No [No] ? y


Now backing up database backend1 in

/export/server71/slapd-marmot/db_backup/backend1.ldif


Shutting down server slapd-marmot . . .

. . . ldiffile: /export/server71/slapd-marmot/db_backup/
backend1.ldif

[14/Apr/2005:17:54:03 -0600] - Waiting for 4 database
threads to stop

[14/Apr/2005:17:54:04 -0600] - All database threads
now stopped


try to reconnect to search cn=backend2,cn=ldbm database,\
cn=plugins,cn=config
```

```
*** LDBM_BACKEND_INSTANCE - cn=backend2,cn=ldbm database,\
cn=plugins,cn=config

already exists

*** Migration will overwrite existing database

Do you want to continue Yes/No [No] ? y

Do you want to export the existing data Yes/No [Yes] ? n

*** INFORMATION - NetscapeRoot is NOT migrated


*** LDBM_BACKEND_INSTANCE - cn=userroot,cn=ldbm database,\
cn=plugins,cn=config

already exists

*** Migration will overwrite existing database

Do you want to continue Yes/No [No] ? n


*** Migration will not update it

----------------------------------------------------------------------

Migrate mapping tree...


*** MAPPING_TREE - cn="dc=example,dc=com",cn=mapping tree,
cn=config already

exists

*** Migration will not add the suffix

----------------------------------------------------------------------

Migrate default indexes...

----------------------------------------------------------------------

Migrate indexes...

----------------------------------------------------------------------

Migrate replicas...

----------------------------------------------------------------------

Migrate replication agreements...

----------------------------------------------------------------------

Migrate Certmap.conf...

Where do you want to back up the file /export/server71/shared/
config/certmap.conf
```

```
[/export/server71/shared/config/certmap.conf_backup] ?

***** Close the LDAP connection to the new Directory Server instance *****

Shutting down server slapd-marmot . . .

. . .

-----------------------------------------------------------------

Data processing...

ldiffile: /export/server621/slapd-marmot/config/ldif/backend1.ldif

[14/Apr/2005:17:56:46 -0600] - Waiting for 4 database threads to stop

[14/Apr/2005:17:56:47 -0600] - All database threads now stopped

ldiffile: /export/server621/slapd-marmot/config/ldif/backend2.ldif

[14/Apr/2005:17:57:22 -0600] - Waiting for 4 database threads to stop

[14/Apr/2005:17:57:23 -0600] - All database threads now stopped

Done.

[14/Apr/2005:17:57:26 -0600] - dblayer_instance_start: pagesize:
4096, pages: 524288, procpages: 1037

[14/Apr/2005:17:57:26 -0600] - cache autosizing: import cache:
204800k

[14/Apr/2005:17:57:26 -0600] - li_import_cache_autosize: 50,
import_pages: 51200, pagesize: 4096

[14/Apr/2005:17:57:26 -0600] - WARNING: Import is running with
nsslapd-db-private-import-mem on; No other process is allowed
to access the database

[14/Apr/2005:17:57:26 -0600] - dblayer_instance_start: pagesize:
4096, pages: 524288, procpages: 1041

[14/Apr/2005:17:57:26 -0600] - cache autosizing: import cache:
204800k

[14/Apr/2005:17:57:26 -0600] - li_import_cache_autosize: 50,
import_pages: 51200, pagesize: 4096

[14/Apr/2005:17:57:27 -0600] - import backend1: Beginning import
job...

[14/Apr/2005:17:57:27 -0600] - import backend1: Index buffering
enabled with bucket size 100

[14/Apr/2005:17:57:27 -0600] - import backend1: Processing file

"/export/server621/slapd-marmot/config/ldif/backend1.ldif"

[14/Apr/2005:17:57:27 -0600] - import backend1: Finished scanning
 file
```

```
"/export/server621/slapd-marmot/config/ldif/backend1.ldif" (1230
entries)

[14/Apr/2005:17:57:27 -0600] - import backend1: Workers finished;
cleaning up...

[14/Apr/2005:17:57:28 -0600] - import backend1: Workers cleaned up.

[14/Apr/2005:17:57:28 -0600] - import backend1: Cleaning up
producer thread...

[14/Apr/2005:17:57:28 -0600] - import backend1: Indexing complete.

Post-processing...

[14/Apr/2005:17:57:28 -0600] - Nothing to do to build ancestorid
index

[14/Apr/2005:17:57:28 -0600] - import backend1: Flushing caches...

[14/Apr/2005:17:57:28 -0600] - import backend1: Closing files...

[14/Apr/2005:17:57:28 -0600] - import backend1: Import complete.
Processed 1230 entries in 4 seconds. (333.51 entries/sec)

[14/Apr/2005:17:57:30 -0600] - dblayer_instance_start: pagesize:
4096, pages: 524288, procpages: 1037

[14/Apr/2005:17:57:30 -0600] - cache autosizing: import cache:
204800k

[14/Apr/2005:17:57:30 -0600] - li_import_cache_autosize: 50,
import_pages: 51200, pagesize: 4096

[14/Apr/2005:17:57:30 -0600] - WARNING: Import is running with
nsslapd-db-private-import-mem on; No other process is allowed to
access the database

[14/Apr/2005:17:57:30 -0600] - dblayer_instance_start: pagesize:
4096, pages:524288, procpages: 1041

[14/Apr/2005:17:57:30 -0600] - cache autosizing: import cache:
204800k

[14/Apr/2005:17:57:30 -0600] - li_import_cache_autosize: 50,
import_pages:

51200, pagesize: 4096

 [14/Apr/2005:17:57:31 -0600] - import backend2: Beginning import
job...

[14/Apr/2005:17:57:31 -0600] - import backend2: Index buffering
enabled withbucket size 100

[14/Apr/2005:17:57:31 -0600] - import backend2: Processing file

"/export/server621/slapd-marmot/config/ldif/backend2.ldif"

[14/Apr/2005:17:57:31 -0600] - import backend2: Finished scanning
file
```

```
"/export/server621/slapd-marmot/config/ldif/backend2.ldif" (0
entries)

[14/Apr/2005:17:57:31 -0600] - import backend2: Workers finished;
cleaning up...

[14/Apr/2005:17:57:31 -0600] - import backend2: Workers cleaned up.

[14/Apr/2005:17:57:31 -0600] - import backend2: Cleaning up
producer thread...

[14/Apr/2005:17:57:31 -0600] - import backend2: Indexing complete.

Post-processing...


[14/Apr/2005:17:57:31 -0600] - Nothing to do to build ancestorid
index

[14/Apr/2005:17:57:31 -0600] - import backend2: Flushing caches...

[14/Apr/2005:17:57:31 -0600] - import backend2: Closing files...

[14/Apr/2005:17:57:32 -0600] - import backend2: Import complete.
Processed 0 entries in 1 seconds. (0.00 entries/sec)

--------------------------------------------------------------------

***** Migrate Changelog...

--------------------------------------------------------------------

***** Migrate ReplicaBindDN entries...

--------------------------------------------------------------------

***** Migrate MultiplexorBindDN entries...


******   End of migration   ******


->  Migration started at Thu Apr 14 23:49:02 2005

->  Migration ended at Thu Apr 14 23:57:44 2005

**********************************************

-> The migration report file is available at:

/export/server71/slapd-marmot//logs/Migration_14042005_174859.log
```

Example 6-1. Sample Output of Directory Server 6.21 to Directory Server 7.1 Migration

6.3.2. Migrating a 6.x Replicated Site

If you are upgrading from Directory Server 6.x to Directory Server 7.x, your replication configuration is automatically migrated when you run the migrateInstance7 script.

To migrate a 6.x replicated site:

1. Stop your Directory Server 6.x.
2. Install Directory Server 7.x.
3. Run the migration script as shown in Section 6.3.1 *Migrating a Standalone Server*.
4. Once your 6.x server is migrated, test replication to make sure it is working correctly.
5. After you finish this process for the master, repeat the steps for the replicas.

6.3.3. Migrating a 6.x Multi-Master Deployment

This section explains how to migrate a deployed *multi-master replication* (MMR) scenario from Directory Server 6.x to Directory Server 7.x. The procedure outlined here ensures that your environment will stay live and no re-initialization will be needed.

Note

If you want to preserve your replication agreements, you must use the same port numbers in your new installations that you used in your legacy servers.

The instructions are written with these assumptions:

- Your deployment consists of separate configuration and standard access instances of Directory Server.
- You are migrating to Directory Server 7.x.

The migration process can be summarized into these steps:

1. Stop directory writes on both masters.

   Warning

   It is imperative that there are no entries being written or changed on the masters during the migration. After both the masters are migrated, writes can resume.

2. After stopping provisioning, make sure all changes have been replicated from the server to migrate to all of its replicas.

   Any changes left over in the changelog will be lost after migration, so make sure all changes in the changelog have been replicated to all replicas.

3. Migrate the first master; refer to Section 6.3.3.1 *Master Migration*.
4. Verify that writes and changes are being replicated through the servers.
5. Migrate the second master; refer toSection 6.3.3.1 *Master Migration*. If required, continue migrating up to four masters.
6. Verify that writes and changes are being replicated through the servers.

7. Migrate the hubs (if any); refer to Section 6.3.3.2 *Hub Migration*.
8. Verify that writes and changes are being replicated through the servers.
9. Migrate the replicas; refer to Section 6.3.3.3 *Replica Migration*.
10. Verify that writes and changes are being replicated through the servers.

6.3.3.1. Master Migration

Follow these steps for the first master, and then repeat the steps for the others, up to four masters.

1. Stop the 6.x Directory Server.
2. Install Directory Server 7.x.

   Make this your configuration instance since it is not replicated. For the other masters, register against the first master's configuration instance.
3. Log into the **Console**, and create a new instance to which you are going to migrate.

   This instance needs to be created to listen on the port that your standard access uses, which is usually 389.
4. Next run the migration script, following the instructions in Section 6.3.1 *Migrating a Standalone Server*.
5. Once your master is migrated, test replication to make sure that it is working correctly.
6. After you finish this process for the first master, repeat the steps for the other masters.

You may wish to set up multi-master replication for `o=NetscapeRoot` between the instances on the masters.

6.3.3.2. Hub Migration

To migrate a 6.x hub:

1. Stop your Directory Server 6.x.
2. Install Directory Server 7.x, registering against the first master's configuration instance.
3. Next run the migration script, following the instructions in Section 6.3.1 *Migrating a Standalone Server*.
4. Once your hub is migrated, test replication to make sure that it is working correctly.
5. After you finish this process for the first hub, repeat the steps for any additional hubs.

6.3.3.3. Replica Migration

To migrate a 6.x replica server:

1. Stop the 6.x Directory Server.
2. Install Directory Server 7.x, registering against the first master's configuration instance.
3. Run the migration script; refer to Section 6.3.1 *Migrating a Standalone Server*.
4. Once your replica is migrated, test replication to make sure that it is working correctly.
5. After you finish this process for the first replica, repeat the steps for any additional replicas.

6.3.4. Managing Console Failover

If you have a multi-master installation with `o=NetscapeRoot` replicated between your two masters, `server1` and `server2`, you can modify the **Console** on the second server (`server2`) so that it uses `server2`'s instance instead of `server1`'s. (By default, writes with `server2`'s **Console** would be made to `server1` then replicated over.)

To accomplish this, you must:

1. Shut down the Administration Server and Directory Server.
2. Change these files to reflect `server2`'s values:
   serverRoot`/userdb/dbswitch.conf:directory default`

   `ldap://`*configHostname*`:`*configPort*`/o%3DNetscapeRoot`

   serverRoot`/admin-serv/config/adm.conf:ldapHost:`*configHostname*

   serverRoot`/admin-serv/config/adm.conf:ldapPort:`*configPort*

   serverRoot`/shared/config/dbswitch.conf:directory default`

   `ldap://`*configHostname*`:`*configPort*`/o%3DNetscapeRoot`

   serverRoot`/slapd-`*serverID*`/config/dse.ldif:nsslapd-pluginarg0:`

   `ldap://`*configHostname*`:`*configPort*`/o%3DnetscapeRoot`
3. Turn off the Pass-through Authentication (PTA) Plug-in on server2 by editing its dse.ldif file.
   a. In a text editor, open this file:
      serverRoot`/slapd-`*serverID*`/config/dse.ldif`
   b. Locate the entry for the PTA plug-in:
      `dn: cn=Pass Through Authentication,cn=plugins,cn=config`
   c. Change nsslapd-pluginEnabled: on to nsslapd-pluginEnabled: off.
   d. Restart the Directory Server and Administration Server.

6.4. Upgrading from Directory Server 7.x Versions

Instead of migrating the Directory Server, you can install an instance of Directory Server 7.1 on top of the Directory Server 7.0 by installing Directory Server 7.1 into the same server root directory. This updates all the server files while preserving your entries and custom schema. These sections explain the upgrade process:

- Section 6.4.1 *Before You Begin*
- Section 6.4.2 *Upgrading*
- Section 6.4.3 *After You Upgrade*.

6.4.1. Before You Begin

Before you begin the upgrade process, back up your entire 7.0 Directory Server. For instructions, check *backing up* and *exporting* in "Populating Directory Databases" in the *Red Hat Directory Server Administration Guide*.

6.4.2. Upgrading

The steps below show how to perform an upgrade using Typical installation:

1. On your Directory Server 7.0 host machine, log in as root or superuser (su).
2. Stop the server.
   `serverRoot/slapd-serverID/stop-server`
3. Create a new directory for the new 7.1 Directory Server. For example:
   ```
   mkdir ds71
   cd ds71
   ```
4. Download the Directory Server product binaries file to the directory you created.
5. Unpack the product binaries file using the following command:
   `gunzip -dc filename.tar.gz | tar -xvof -`

   where *filename* corresponds to the product binaries that you want to unpack.
6. In the list of files, locate the setup program.
7. Run the setup program by issuing the following command from the installation directory:
   `./setup`

   The setup program asks if you would like to proceed with the setup.
8. Press [Enter] to respond with the default (the default for this prompt is **Yes**) or press **n** if you would like to exit the setup program.
9. Next, the setup program asks you if you agree to the license terms. Press **y** to agree with the license terms.
10. When you are asked what you would like to install, press **Enter** to select the default, Red Hat Servers.
11. When you are asked what type of installation you would like to perform, press **Enter** to select the default, `Typical Installation`.
12. When prompted to enter the server root (or the installation directory), enter the full path to the location where your Directory Server 7.0 is installed.

    By default, the setup program provides the following path:
    `/opt/redhat-ds/servers`

    If your 7.0 Directory Server is installed in a different path, be sure to select that path. Once you supply the correct path, press [Enter].
13. The setup program starts upgrading your server. Follow the prompts, and complete the upgrade process.

6.4.3. After You Upgrade

To verify that the upgrade process was successful, check the upgraded server for data consistency and any custom schema.

Chapter 7.
Troubleshooting

This chapter describes the most common installation problems and how to solve them. It also provides some tips on checking patch levels and kernel parameter settings for your system.

This chapter has the following sections:

- Section 7.1 *Running* `dsktune`
- Section 7.2 *Common Installation Problems*

7.1. Running `dsktune`

The `dsktune` utility provides an easy and reliable way of checking the patch levels and kernel parameter settings for your system. You must install the Directory Server before you can run `dsktune`.

On Solaris platforms, if you run the `dsktune` utility, it reports as missing any of the patches from the Sun recommended patch list that are not installed on your system, even if they relate to packages that you have not installed.

To run `dsktune`:

1. Change to the installation directory for your Directory Server.

   By default, this directory is /opt/redhat-ds/servers.
2. Change to the bin/slapd/server subdirectory.
3. As root, enter the following command:
   `./dsktune`

The following is an example of output that `dsktune` generates. `dsktune` does not itself make any changes to the system.

```
Executing /tmp/redhat/dsktune...

Red Hat Directory Server system tuning analysis version
04-APRIL-2005.

NOTICE : System is hppa2.0/549-hp9000/785/J5000-hpux_B.11.11.

WARNING : Only the superuser can check which patches are installed.
 You must run
dsktune as root to ensure the necessary patches are present.
 If required patches
are not present, the server may not function correctly.

NOTICE : The tcp_keepalive_interval is set to 7200000 milliseconds
(120 minutes).

This may cause temporary server congestion from lost client
connections.

An entry similar to the following should be added to
/etc/rc.config.d/nddconf:
```

```
TRANSPORT_NAME[10]=tcp

NDD_NAME[10]=tcp_keepalive_interval

NDD_VALUE[10]=600000

NOTICE : The NDD tcp_rexmit_interval_initial is currently set to
3000 milliseconds (3 seconds).
 This may cause packet loss for clients on Solaris
2.5.1 due to a bug in that version of Solaris.
 If the clients are not using
Solaris 2.5.1, no problems should occur.

NOTICE : If the directory service is intended only for LAN or
private high-speed WAN environment, this interval can be reduced
by adding an entry similar to the following to
/etc/rc.config.d/nddconf file:

TRANSPORT_NAME[10]=tcp

NDD_NAME[10]=tcp_rexmit_interval_initial

NDD_VALUE[10]=500

NOTICE : The NDD tcp_ip_abort_cinterval is currently set to 75000
milliseconds (75 seconds).
 This may cause long delays in establishing outgoing connections if
the destination server is down.

NOTICE : If the directory service is intended only for LAN or
private high-speed WAN environment, this interval can be reduced
by adding an entry similar to the following to
/etc/rc.config.d/nddconf file:

TRANSPORT_NAME[10]=tcp

NDD_NAME[10]=tcp_ip_abort_cinterval

NDD_VALUE[10]=10000

NOTICE : The NDD tcp_ip_abort_interval is currently set to 75000
milliseconds (75 seconds).
 This may cause long delays in detecting connection failure if the
destination server is down.

NOTICE : If the directory service is intended only for LAN or
private high-speed WAN environment, this interval can be reduced
by adding an entry similar to the following to
/etc/rc.config.d/nddconf file:

TRANSPORT_NAME[10]=tcp

NDD_NAME[10]=tcp_ip_abort_interval

NDD_VALUE[10]=60000

ERROR  : The NDD tcp_smallest_anon_port is currently 49152.
 This allows a maximum
of 16384 simultaneous connections.
 More ports can be made available by adding an
entry similar to the following to /etc/rc.config.d/nddconf:
```

```
TRANSPORT_NAME[10]=tcp

NDD_NAME[10]=tcp_smallest_anon_port

NDD_VALUE[10]=8192

WARNING: tcp_deferred_ack_interval is currently 50 milliseconds.
This will cause the operating system to insert artificial delays
in the LDAP protocol.
 It should be reduced during load testing.
An entry similar to the following can be added to
the /etc/rc.config.d/nddconf file:

TRANSPORT_NAME[10]=tcp

NDD_NAME[10]=tcp_deferred_ack_interval

NDD_VALUE[10]=5

WARNING: largefiles option is not present on mount of /opt,
although it is present on other file systems.
 Files on the /opt file system will be limited to 2GB in
size.

NOTICE : /opt partition has only 90MB free.

Continue [n]?
```

Example 7-1. Sample `dsktune` Output

7.2. Common Installation Problems

Clients cannot locate the server

First, try using the host name. If that does not work, use the fully qualified name (such as www.domain.com), and make sure the server is listed in the DNS. If that does not work, use the IP address.

If your NIS domain is different from your DNS domain, the fully-qualified host and domain name presented by the installer may be incorrect. These values must be corrected to use the DNS domain name.

The port is in use

You probably did not shut down a server before you upgraded it. Shut down the old server, then manually start the upgraded one.

Another installed server might be using the port. Make sure the port you have chosen is not already being used by another server.

LDAP authentication error causes install to fail

If you are installing Directory Server in a network that uses NIS naming rather than DNS naming, you may get the following error, with *`incorrect.DNS.address`* replaced by the DNS address you attempted to use:

```
ERROR: Ldap authentication failed for url
ldap://incorrect.DNS.address
```

```
user id admin (151:Unknown error.)

Fatal Slapd Did not add Directory Server information to
Configuration Server.

ERROR.
Failure installing Red Hat Directory Server.
Do you want to
continue [y/n]?
```

This error occurs when a machine is not correctly configured to use DNS naming. The default fully qualified host and domain name presented during installation is not correct. If you accept the defaults, you receive the LDAP authentication error.

To install successfully, you need to provide a fully qualified domain name that consists of a local host name along with its domain name. A host name is the logical name assigned to a computer. For example, `mycomputer` is a host name and `example.com` is a *fully qualified domain name* (FQDN).

A fully qualified domain name should be sufficient to determine a unique Internet address for any host on the Internet. The same naming scheme is also used for some hosts that are not on the Internet but share the same namespace for electronic mail addressing.

"Failure (4322): Configuration initialization failed" error message on Linux

`libjvm.so` (from JRE 1.4), which the Administration Server uses to run servlets, requires that the `compat-libstdc++-6.2` package be installed when running the server on Red Hat Enterprise Linux.

The package may or may not be installed depending on the options that were chosen when the operating system was installed. If the package is not installed, you get an error similar to the one in Example 7-2.

```
[18/Jun/2002:10:56:39] failure ( 4322): Configuration
initialization failed:

Error running init function load-modules: dlopen of
/export/dstest/bin/https/lib/libNSServletPlugin.so failed

(libstdc++-libc6.1-1.so.2: cannot open shared object file:
No such file or directory)
```

Example 7-2. Error — Missing `libstdc++` Package

For more information on the Sun supplied package, check the JRE's release notes at http://java.sun.com/j2se/1.4/install-linux.html.

Forgotten Directory manager DN and password

If you forget the manager DN, you can find out what the Directory Manager DN is by looking for the *`nsslapd-rootdn`* attribute in the file *`serverRoot`*`/slapd-`*`serverID`*`/config/dse.ldif`.

If you have forgotten the Directory Manager DN password, you can reset it by doing the following:

1. Find the *`nsslapd-rootpw`* attribute in `slapd.conf`. If the attribute value is not encrypted in any way (that is, it does not start with `{SHA}` or `{CRYPT}`), then the password is exactly what is shown on the parameter.
2. If the attribute is encrypted, then delete the attribute value, and replace it with some cleartext value. For example, if you change the *`nsslapd-rootpw`* attribute so that it is:
   `nsslapd-rootpw: my_password`

then your Directory Manager DN password is now `my_password`.

3. Restart your Directory Server.
4. Once your server has restarted, login as the Directory Manager and change the password. Make sure you select an encryption scheme when you do so.

For information on changing a Directory Manager password, refer to the *Red Hat Directory Server Administration Guide*.

Is there a way to debug Directory Server installation and uninstallation problems?

Some problems may develop when you uninstall Directory Server and then reinstall. Logging has been enhanced to report setup and uninstall problems with detailed error messages to provide you with enough information to fix the problem. The setup log file is located in the following path: *`serverRoot`*`/setup/setup.log`. The uninstall log file, uninst.log, is stored in the system TEMP directory. This directory is usually `/tmp` or `/var/tmp`.

Glossary

A

access control instruction

See *ACI*.

ACI

Access Control Instruction. An instruction that grants or denies permissions to entries in the directory.

access control list

See *ACL*.

ACL

Access Control List. The mechanism for controlling access to your directory.

access rights

In the context of access control, specify the level of access granted or denied. Access rights are related to the type of operation that can be performed on the directory. The following rights can be granted or denied: read, write, add, delete, search, compare, selfwrite, proxy and all.

account inactivation

Disables a user account, group of accounts, or an entire domain so that all authentication attempts are automatically rejected.

All IDs Threshold

A size limit which is globally applied to every index key managed by the server. When the size of an individual ID list reaches this limit, the server replaces that ID list with an All IDs token.

All IDs token

A mechanism which causes the server to assume that all directory entries match the index key. In effect, the All IDs token causes the server to behave as if no index were available for the search request.

anonymous access

When granted, allows anyone to access directory information without providing credentials, and regardless of the conditions of the bind.

approximate index

Allows for efficient approximate or "sounds-like" searches.

attribute

Holds descriptive information about an entry. Attributes have a label and a value. Each attribute also follows a standard syntax for the type of information that can be stored as the attribute value.

attribute list

A list of required and optional attributes for a given entry type or object class.

authenticating directory server

In pass-through authentication (PTA), the authenticating Directory Server is the Directory Server that contains the authentication credentials of the requesting client. The PTA-enabled host sends PTA requests it receives from clients to the host.

authentication

(1) Process of proving the identity of the client user to the Directory Server. Users must provide a bind DN and either the corresponding password or certificate in order to be granted access to the directory. Directory Server allows the user to perform functions or access files and directories based on the permissions granted to that user by the directory administrator.

(2) Allows a *client* to make sure they are connected to a secure server, preventing another computer from impersonating the server or attempting to appear secure when it is not.

authentication certificate

Digital file that is not transferable, cannot be forged, and is issued by a third party. Authentication certificates are sent from server to client or client to server in order to verify and authenticate the other party.

B

base DN

Base distinguished name. A search operation is performed on the base DN, the DN of the entry and all entries below it in the directory tree.

base distinguished name

See *base DN*.

bind DN

Distinguished name used to authenticate to Directory Server when performing an operation.

bind distinguished name

See *bind DN*.

bind rule

In the context of access control, the bind rule specifies the credentials and conditions that a particular user or client must satisfy in order to get access to directory information.

branch entry

An entry that represents the top of a subtree in the directory.

browser

Software, such as Mozilla Firefox, used to request and view World Wide Web material stored as HTML files. The browser uses the HTTP protocol to communicate with the host server.

browsing index

Also *virtual view index*. Speeds up the display of entries in the Directory Server Console. Browsing indexes can be created on any branchpoint in the directory tree to improve display performance.

C

CA

See *Certificate Authority*.

cascading replication

In a cascading replication scenario, one server, often called the hub supplier, acts both as a consumer and a supplier for a particular replica. It holds a read-only replica and maintains a changelog. It receives updates from the supplier server that holds the master copy of the data and in turn supplies those updates to the consumer.

certificate

A collection of data that associates the public keys of a network user with their DN in the directory. The certificate is stored in the directory as user object attributes.

Certificate Authority

Company or organization that sells and issues authentication certificates. You may purchase an authentication certificate from a Certification Auth

CGI

Common Gateway Interface. An interface for external programs to communicate with the HTTP server. Programs written to use CGI are called CGI programs or CGI scripts and can be written in many of the common programming languages. CGI programs handle forms or perform output parsing that is not done by the server itself.

chaining

A method for relaying requests to another server. Results for the request are collected, compiled, and then returned to the client.

changelog

A changelog is a record that describes the modifications that have occurred on a replica. The supplier server then replays these modifications on the replicas stored on consumer servers or on other masters, in the case of multi-master replication.

character type

Distinguishes alphabetic characters from numeric or other characters and the mapping of upper-case to lower-case letters.

ciphertext

Encrypted information that cannot be read by anyone without the proper key to decrypt the information.

CIR

See *consumer-initiated replication*.

class definition

Specifies the information needed to create an instance of a particular object and determines how the object works in relation to other objects in the directory.

class of service

See *CoS*.

classic CoS

A classic CoS identifies the template entry by both its DN and the value of one of the target entry's attributes.

client

See *LDAP client*.

code page

An internal table used by a locale in the context of the internationalization plug-in that the operating system uses to relate keyboard keys to character font screen displays.

collation order

Provides language and cultural-specific information about how the characters of a given language are to be sorted. This information might include the sequence of letters in the alphabet or how to compare letters with accents to letters without accents.

consumer

Server containing replicated directory trees or subtrees from a supplier server.

consumer-initiated replication

Replication configuration where *consumer* servers pull directory data from supplier servers.

consumer server

In the context of replication, a server that holds a replica that is copied from a different server is called a consumer for that replica.

CoS

A method for sharing attributes between entries in a way that is invisible to applications.

CoS definition entry

Identifies the type of CoS you are using. It is stored as an LDAP subentry below the branch it affects.

CoS template entry

Contains a list of the shared attribute values. Also template entry.

D

daemon

A background process on a UNIX machine that is responsible for a particular system task. Daemon processes do not need human intervention to continue functioning.

DAP

Directory Access Protocol. The ISO X.500 standard protocol that provides client access to the directory.

data master

The server that is the master source of a particular piece of data.

database link

An implementation of chaining. The database link behaves like a database but has no persistent storage. Instead, it points to data stored remotely.

default index

One of a set of default indexes created per database instance. Default indexes can be modified, although care should be taken before removing them, as certain plug-ins may depend on them.

definition entry

See *CoS definition entry*.

Directory Access Protocol

See *DAP*.

directory tree

The logical representation of the information stored in the directory. It mirrors the tree model used by most filesystems, with the tree's root point appearing at the top of the hierarchy. Also known as *DIT*.

Directory Manager

The privileged database administrator, comparable to the root user in UNIX. Access control does not apply to the Directory Manager.

Directory Server Gateway

Also DSGW. A collection of CGI forms that allows a browser to perform LDAP client functions, such as querying and accessing a Directory Server, from a web browser.

directory service

A database application designed to manage descriptive, attribute-based information about people and resources within an organization.

distinguished name

String representation of an entry's name and location in an LDAP directory.

DIT

See *directory tree*.

DN

See *distinguished name*.

DM

See *Directory Manager*.

DNS

Domain Name System. The system used by machines on a network to associate standard IP addresses (such as 198.93.93.10) with hostnames (such as www.example.com). Machines normally get the IP address for a hostname from a DNS server, or they look it up in tables maintained on their systems.

DNS alias

A DNS alias is a hostname that the DNS server knows points to a different host-specifically a DNS CNAME record. Machines always have one real name, but they can have one or more aliases. For example, an alias such as www. *yourdomain.domain* might point to a real machine called realthing. *yourdomain.domain* where the server currently exists.

DSGW

See *Directory Server Gateway*.

E

entry

A group of lines in the LDIF file that contains information about an object.

entry distribution

Method of distributing directory entries across more than one server in order to scale to support large numbers of entries.

entry ID list

Each index that the directory uses is composed of a table of index keys and matching entry ID lists. The entry ID list is used by the directory to build a list of candidate entries that may match the client application's search request.

equality index

Allows you to search efficiently for entries containing a specific attribute value.

F

file extension

The section of a filename after the period or dot (.) that typically defines the type of file (for example, .GIF and .HTML). In the filename index.html the file extension is html.

file type

The format of a given file. For example, graphics files are often saved in GIF format, while a text file is usually saved as ASCII text format. File types are usually identified by the file extension (for example, .GIF or .HTML).

filter

A constraint applied to a directory query that restricts the information returned.

filtered role

Allows you to assign entries to the role depending upon the attribute contained by each entry. You do this by specifying an LDAP filter. Entries that match the filter are said to possess the role.

G

gateway

See *Directory Server Gateway*.

general access

When granted, indicates that all authenticated users can access directory information.

GSS-API

Generic Security Services. The generic access protocol that is the native way for UNIX-based systems to access and authenticate Kerberos services; also supports session encryption.

H

hostname

A name for a machine in the form machine.domain.dom, which is translated into an IP address. For example, www.example.com is the machine www in the subdomain example and com domain.

HTML

Hypertext Markup Language. The formatting language used for documents on the World Wide Web. HTML files are plain text files with formatting codes that tell browsers such as the Mozilla Firefox how to display text, position graphics, and form items and to display links to other pages.

HTTP

Hypertext Transfer Protocol. The method for exchanging information between HTTP servers and clients.

HTTPD

An abbreviation for the HTTP daemon or service, a program that serves information using the HTTP protocol. The daemon or service is often called an httpd.

HTTP-NG

The next generation of Hypertext Transfer Protocol.

HTTPS

A secure version of HTTP, implemented using the Secure Sockets Layer, SSL.

hub supplier

In the context of replication, a server that holds a replica that is copied from a different server, and, in turn, replicates it to a third server. See also cascading replication.

I

index key

Each index that the directory uses is composed of a table of index keys and matching entry ID lists.

indirect CoS

An indirect CoS identifies the template entry using the value of one of the target entry's attributes.

international index

Speeds up searches for information in international directories.

IP address

Also Internet Protocol address. A set of numbers, separated by dots, that specifies the actual location of a machine on the Internet (for example, 198.93.93.10).

ISO

International Standards Organization.

K

knowledge reference

Pointers to directory information stored in different databases.

L

LDAP

Lightweight Directory Access Protocol. Directory service protocol designed to run over TCP/IP and across multiple platforms.

LDAPv3

Version 3 of the LDAP protocol, upon which Directory Server bases its schema format.

LDAP client

Software used to request and view LDAP entries from an LDAP Directory Server. See also *browser*.

LDAP Data Interchange Format

See *LDAP Data Interchange Format*.

LDAP URL

Provides the means of locating Directory Servers using DNS and then completing the query via LDAP. A sample LDAP URL is ldap://ldap.example.com.

LDBM database

A high-performance, disk-based database consisting of a set of large files that contain all of the data assigned to it. The primary data store in Directory Server.

LDIF

LDAP Data Interchange Format. Format used to represent Directory Server entries in text form.

leaf entry

An entry under which there are no other entries. A leaf entry cannot be a branch point in a directory tree.

Lightweight Directory Access Protocol

See *LDAP*.

locale

Identifies the collation order, character type, monetary format and time / date format used to present data for users of a specific region, culture, and/or custom. This includes information on how data of a given language is interpreted, stored, or collated. The locale also indicates which code page should be used to represent a given language.

M

managed object

A standard value which the SNMP agent can access and send to the NMS. Each managed object is identified with an official name and a numeric identifier expressed in dot-notation.

managed role

Allows creation of an explicit enumerated list of members.

management information base

See *MIB*.

mapping tree

A data structure that associates the names of suffixes (subtrees) with databases.

master agent

See *SNMP master agent*.

master server

The server that contains the master copy of the directory trees or subtrees that are replicated to replicas. The master server is read-write.

matching rule

Provides guidelines for how the server compares strings during a search operation. In an international search, the matching rule tells the server what collation order and operator to use.

MD5

A message digest algorithm by RSA Data Security, Inc., which can be used to produce a short digest of data that is unique with high probability and is mathematically extremely hard to produce; a piece of data that will produce the same message digest.

MD5 signature

A message digest produced by the MD5 algorithm.

MIB

Management Information Base. All data, or any portion thereof, associated with the SNMP network. We can think of the MIB as a database which contains the definitions of all SNMP managed objects. The MIB has a tree-like hierarchy, where the top level contains the most general information about the network and lower levels deal with specific, separate network areas.

MIB namespace

Management Information Base namespace. The means for directory data to be named and referenced. Also called the directory tree.

monetary format

Specifies the monetary symbol used by specific region, whether the symbol goes before or after its value, and how monetary units are represented.

multi-master replication

An advanced replication scenario in which two servers each hold a copy of the same read-write replica. Each server maintains a changelog for the replica. Modifications made on one server are automatically replicated to the other server. In case of conflict, a time stamp is used to determine which server holds the most recent version.

multiplexor

The server containing the database link that communicates with the remote server.

N

n + 1 directory problem

The problem of managing multiple instances of the same information in different directories, resulting in increased hardware and personnel costs.

name collisions

Multiple entries with the same distinguished name.

nested role

Allows the creation of roles that contain other roles.

network management application

Network Management Station component that graphically displays information about SNMP managed devices (which device is up or down, which and how many error messages were received, etc.).

network management station

See *NMS*.

NIS

Network Information Service. A system of programs and data files that UNIX machines use to collect, collate, and share specific information about machines, users, filesystems, and network parameters throughout a network of computers.

NMS

Also Network Management Station. Powerful workstation with one or more network management applications installed.

ns-slapd

Red Hat's LDAP Directory Server daemon or service that is responsible for all actions of the Directory Server. See also *slapd*.

O

object class

Defines an entry type in the directory by defining which attributes are contained in the entry.

object identifier

Also OID. A string, usually of decimal numbers, that uniquely identifies a schema element, such as an object class or an attribute, in an object-oriented system. Object identifiers are assigned by ANSI, IETF or similar organizations.

OID

See *object identifier*.

operational attribute

Contains information used internally by the directory to keep track of modifications and subtree properties. Operational attributes are not returned in response to a search unless explicitly requested.

P

parent access

When granted, indicates that users have access to entries below their own in the directory tree if the bind DN is the parent of the targeted entry.

pass-through authentication

See *PTA*.

pass-through subtree

In pass-through authentication, the *PTA directory server* will pass through bind requests to the *authenticating directory server* from all clients whose DN is contained in this subtree.

password file

A file on UNIX machines that stores UNIX user login names, passwords, and user ID numbers. It is also known as /etc/passwd because of where it is kept.

password policy

A set of rules that governs how passwords are used in a given directory.

permission

In the context of access control, permission states whether access to the directory information is granted or denied and the level of access that is granted or denied. See access rights.

PDU

Also Protocol Data Unit. Encoded messages which form the basis of data exchanges between SNMP devices.

pointer CoS

A pointer CoS identifies the template entry using the template DN only.

presence index

Allows searches for entries that contain a specific indexed attribute.

protocol

A set of rules that describes how devices on a network exchange information.

protocol data unit

See *PDU*.

proxy authentication

A special form of authentication where the user requesting access to the directory does not bind with its own DN but with a proxy DN.

proxy DN

Used with proxied authorization. The proxy DN is the DN of an entry that has access permissions to the target on which the client-application is attempting to perform an operation.

PTA

Also Pass-through authentication. Mechanism by which one Directory Server consults another to check bind credentials.

PTA directory server

In pass-through authentication (*PTA*), the PTA Directory Server is the server that sends (passes through) bind requests it receives to the *authenticating directory server*.

PTA LDAP URL

In pass-through authentication, the URL that defines the *authenticating directory server*, pass-through subtree(s), and optional parameters.

R

RAM

Random access memory. The physical semiconductor-based memory in a computer. Information stored in RAM is lost when the computer is shut down.

rc.local

A file on UNIX machines that describes programs that are run when the machine starts. It is also called /etc/rc.local because of its location.

RDN

Also Relative Distinguished Name. The name of the actual entry itself, before the entry's ancestors have been appended to the string to form the full distinguished name.

referential integrity

Mechanism that ensures that relationships between related entries are maintained within the directory.

referral

(1) When a server receives a search or update request from an LDAP client that it cannot process, it usually sends back to the client a pointer to the LDAP sever that can process the request.

(2) In the context of replication, when a read-only replica receives an update request, it forwards it to the server that holds the corresponding read-write replica. This forwarding process is called a referral.

replica

A database that participates in replication.

read-only replica

A replica that refers all update operations to read-write replicas. A server can hold any number of read-only replicas.

read-write replica

A replica that contains a master copy of directory information and can be updated. A server can hold any number of read-write replicas.

relative distinguished name

See *RDN*.

replication

Act of copying directory trees or subtrees from supplier servers to consumer servers.

replication agreement

Set of configuration parameters that are stored on the supplier server and identify the databases to replicate, the consumer servers to which the data is pushed, the times during which replication can occur, the DN and credentials used by the supplier to bind to the consumer, and how the connection is secured.

RFC

Request for Comments. Procedures or standards documents submitted to the Internet community. People can send comments on the technologies before they become accepted standards.

role

An entry grouping mechanism. Each role has *members*, which are the entries that possess the role.

role-based attributes

Attributes that appear on an entry because it possesses a particular role within an associated CoS template.

root

The most privileged user available on UNIX machines. The root user has complete access privileges to all files on the machine.

root suffix

The parent of one or more sub suffixes. A directory tree can contain more than one root suffix.

S

SASL

Also Simple Authentication and Security Layer. An authentication framework for clients as they attempt to bind to a directory.

schema

Definitions describing what types of information can be stored as entries in the directory. When information that does not match the schema is stored in the directory, clients attempting to access the directory may be unable to display the proper results.

schema checking

Ensures that entries added or modified in the directory conform to the defined schema. Schema checking is on by default, and users will receive an error if they try to save an entry that does not conform to the schema.

Secure Sockets Layer

See *SSL*.

self access

When granted, indicates that users have access to their own entries if the bind DN matches the targeted entry.

Server Console

Java-based application that allows you to perform administrative management of your Directory Server from a GUI.

server daemon

The server daemon is a process that, once running, listens for and accepts requests from clients.

server root

A directory on the server machine dedicated to holding the server program and configuration, maintenance, and information files.

Server Selector

Interface that allows you select and configure servers using a browser.

service

A background process on a Windows machine that is responsible for a particular system task. Service processes do not need human intervention to continue functioning.

SIE

Server Instance Entry. The ID assigned to an instance of Directory Server during installation.

Simple Authentication and Security Layer

See SASL.

Simple Network Management Protocol

See *SNMP*.

single-master replication

The most basic replication scenario in which two servers each hold a copy of the same read-write replicas to consumer servers. In a single-master replication scenario, the supplier server maintains a changelog.

SIR

See *supplier-initiated replication*.

slapd

LDAP Directory Server daemon or service that is responsible for most functions of a directory except replication. See also *ns-slapd*.

SNMP

Also Simple Network Management Protocol. Used to monitor and manage application processes running on the servers by exchanging data about network activity.

SNMP master agent

Software that exchanges information between the various subagents and the NMS.

SNMP subagent

Software that gathers information about the managed device and passes the information to the master agent. Also subagent.

SSL

Also Secure Sockets Layer. A software library establishing a secure connection between two parties (client and server) used to implement HTTPS, the secure version of HTTP.

standard index

index maintained by default.

sub suffix

A branch underneath a root suffix.

subagent

See *SNMP subagent*.

substring index

Allows for efficient searching against substrings within entries. Substring indexes are limited to a minimum of two characters for each entry.

suffix

The name of the entry at the top of the directory tree, below which data is stored. Multiple suffixes are possible within the same directory. Each database only has one suffix.

superuser

The most privileged user available on UNIX machines. The superuser has complete access privileges to all files on the machine. Also called root.

supplier

Server containing the master copy of directory trees or subtrees that are replicated to consumer servers.

supplier server

In the context of replication, a server that holds a replica that is copied to a different server is called a supplier for that replica.

supplier-initiated replication

Replication configuration where *supplier* servers replicate directory data to consumer servers.

symmetric encryption

Encryption that uses the same key for both encrypting and decrypting. DES is an example of a symmetric encryption algorithm.

system index

Cannot be deleted or modified as it is essential to Directory Server operations.

T

target

In the context of access control, the target identifies the directory information to which a particular ACI applies.

target entry

The entries within the scope of a CoS.

TCP/IP

Transmission Control Protocol/Internet Protocol. The main network protocol for the Internet and for enterprise (company) networks.

template entry

See *CoS template entry*.

time/date format

Indicates the customary formatting for times and dates in a specific region.

TLS

Also Transport Layer Security. The new standard for secure socket layers; a public key based protocol.

topology

The way a directory tree is divided among physical servers and how these servers link with one another.

Transport Layer Security

See *TLS*.

U

uid

A unique number associated with each user on a UNIX system.

URL

Uniform Resource Locator. The addressing system used by the server and the client to request documents. It is often called a location. The format of a URL is `protocol://machine:port/document`. The port number is necessary only on selected servers, and it is often assigned by the server, freeing the user of having to place it in the URL.

V

virtual list view index

Also browsing index. Speeds up the display of entries in the Directory Server Console. Virtual list view indexes can be created on any branchpoint in the directory tree to improve display performance.

X

X.500 standard

The set of ISO/ITU-T documents outlining the recommended information model, object classes and attributes used by directory server implementation.

Index

Symbols

32-bit OS requirements, 9
32-bit process, 9
64-bit OS requirements, 10
64-bit process, 10

A

administration domain, defined, 5
administration port number, setting, 26, 29
administration server, 1
administration server user, 4
authentication entities, 3

B

browsing index, 67

C

classic CoS, 69
configuration decisions, 1
configuration directory administrator, 4
configuration directory, defined, 4
Console, 1
creating instances under the same server root, 31
custom install, defined, 7

D

default server root, 2
directory tree
  configuring, 44
directory manager, 4
directory server, i, 1
directory suffix, 4
dsktune utility, 12
ds_create
  creates new DS instance, 41

E

express install
  defined, 6
express install
  using, 23

H

help
  launching, 43

I

install.inf, 32
installation
  components, 1
  configuration decisions, 1
  preparing for, 1
  process overview
    new installations, 7
  requirements, 9
installation overview
  Red Hat Enterprise Linux, 12
installation process
  selecting, 6
installation process
  overview, 6
installation directory, default, 3
installation overview
  HP-UX 11i, 15
  Solaris 9, 17
installation process
  privileges required for, 8

L

LDAP Data Interchange Format (LDIF)
  creating databases using, 44

M

migrating
  6.x MMR deployment, 54
  6.x replicated sites, 54
  standalone server, 47
migration
  defined, 45
  overview, 45
  prerequisites, 46
  procedure, 46
migration process
  overview, 7

N

new server root
  creating, 2
nobody user account, 3
ns-slapd process
  write an rc script for, 8

O

operating systems, supported, 9

P

port numbers
  choosing unique, 2
  troubleshooting, 61
PrePreInstall field, 12
prerequisites
  migration, 46

R

Red Hat Administration Server, 1
Red Hat Console, 1
replicated site
  migration of 6.x MMR deployment, 54
  migration of 6.x sites, 54
requirements
  computer hardware, 11
  computer system, 9
  disk space, HP-UX, 15
  disk space, Red Hat Enterprise Linux, 13
  disk space, Solaris, 17
  DNS and NIS, 20
  operating system, 12
  system modules, Red Hat Enterprise Linux, 13
  system patches, Red Hat Enterprise Linux, 14
root directory tree, 4
root DN (directory manager), 4

S

server root, 2
setup program, using from command line, 31
silent install
  defined, 7
silent install
  creating install files, 32
  directives
    admin, 39
    base, 40
    general, 36
    nsperl, 40
    perldap, 40
    slapd, 37
  typical install example, 33
  using, 31
supported platforms, 9
system tuning, Red Hat Enterprise Linux, 14

T

third-party utilities
  installing, Red Hat Enterprise Linux, 15
typical install
  defined, 6

U

upgrade
  prerequisites, 57
user and groups to run servers as, 3
user directory, defined, 5